IP Security (IPSec)

IPSec

When two devices want to communicate securely, they must set up a secure path between themselves. But, this path may traverse across many insecure intermediate devices/ systems. Thus, the two devices must

- Agree on a set of security protocols that standardize the data format
- Decide upon an encryption algorithm
- Exchange keys

IPsec is a group of protocols that are used together to set up encrypted connections between devices. It helps secure data sent over public networks and is often used to set up VPNs. It works by encrypting IP packets, along with authenticating the source where the packets come from.

IPSec

- IPSec provides
  - Access control: User authentication
  - Data integrity
  - Data origin authentication
  - Rejection of replayed packets
  - Confidentiality – by encrypting data

- Benefits:
  - Operates at Layer 3 and has no impact on higher layers. Hence, it is transparent to applications and end users need not bother about its configuration
  - Applies to all transports/applications
  - When implemented in Firewall/router, it provides security to all traffic crossing the perimeter
  - Can provide security for individual users

- Applications: VPNs, Branch Offices, Remote Users, Extranets

IPSec services

IPsec core protocols:

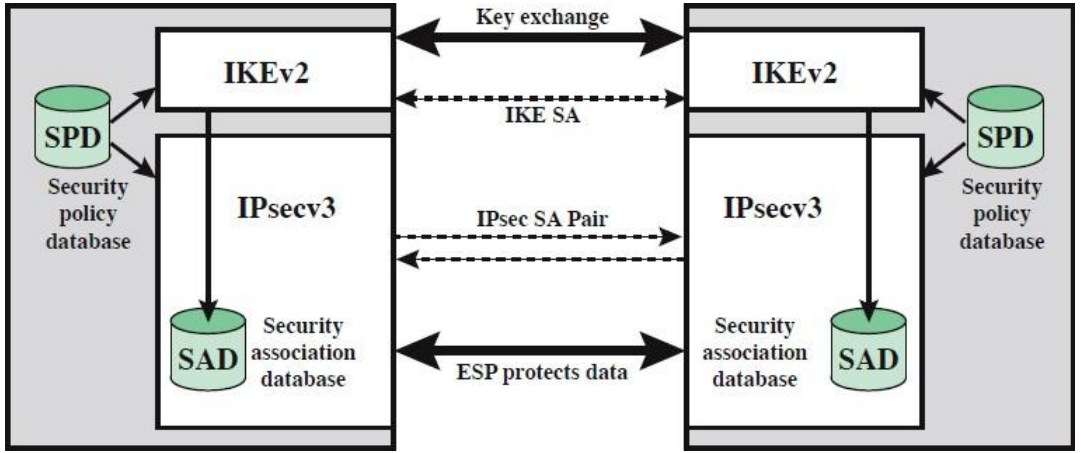
- **Authentication Header (AH)** – ensures data integrity and replay attack protection
- **Encapsulating Security Payload (ESP)** – allows encryption to ensure data authentication

Services	*AH*	*ESP*
Access control	Yes	Yes
Message authentication (message integrity)	Yes	Yes
Entity authentication (data source authentication)	Yes	Yes
Confidentiality	No	Yes
Replay attack protection	Yes	Yes

- **Access Control** – provides indirect access control through SAD
- **Message Authentication** – message integrity is preserved in both AH and ESP
- **Entity Authentication** – SA along with key-hashed message digest helps authenticate the sender in both AH and ESP
- **Confidentiality** – Encryption in ESP provides confidentiality
- **Replay Attack Protection** – Both AH and ESP prevent replay attack by using sequence numbers

IPSec Architecture

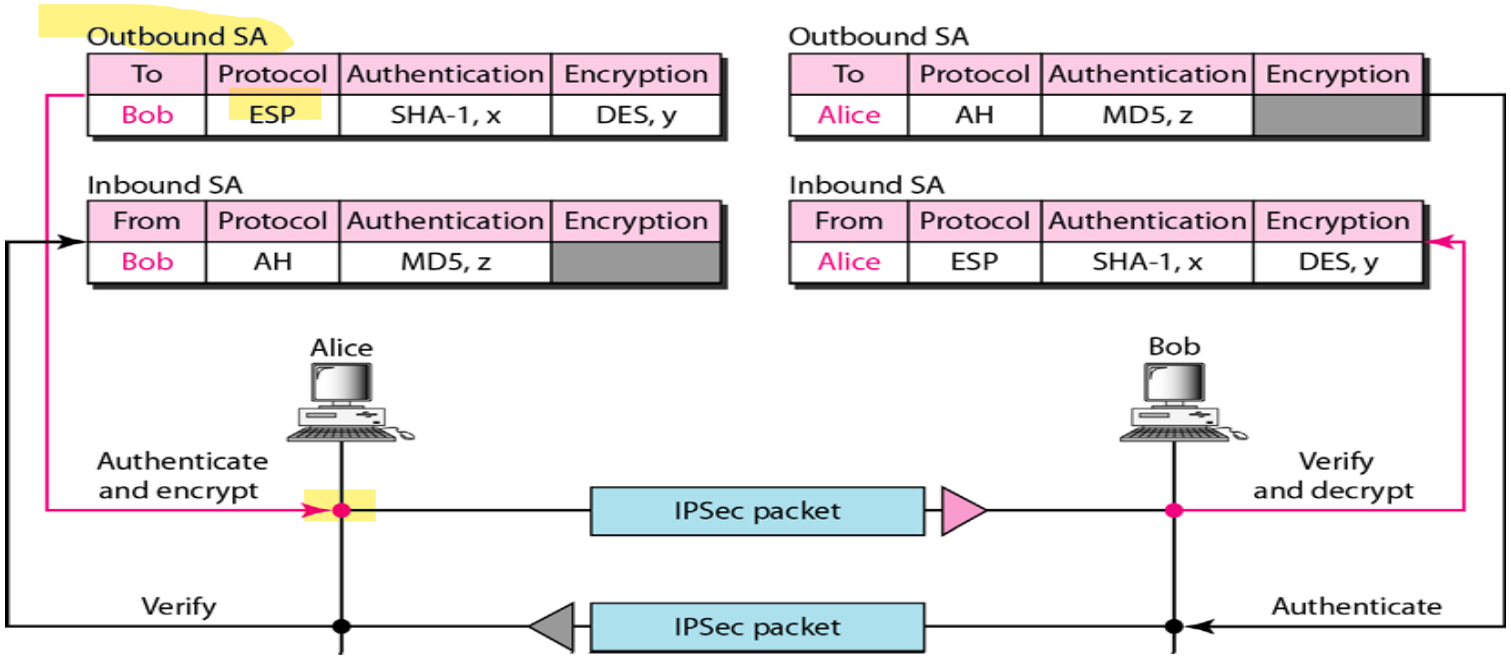
- Internet Key Exchange (IKE)
- IPSec
- Security Association Database
- Security Policy Database



Security Association (SA) Database

- A security association (SA) is a one-way logical connection between a sender and a receiver that specifies the security properties recognized by the communicating hosts.
- A pair of hosts typically require two SAs to communicate securely in both directions, as a single SA protects data in one direction. SAs are needed for the encryption-decryption processes to negotiate a security level between two hosts.
- SAs are stored in a Security Association Database (SAD). Each host has a SAD.
- A SA is defined by 3 parameters:
  - Security Parameters Index (SPI) - an integer that specifies the row in the SAD that a receiver should use to decrypt a received packet
  - IP Destination Address
  - Security Protocol: AH or ESP
- For each SA, the database contains:
  - SPI, Sequence number counter and counter overflow flag, Anti-replay window, AH Information and ESP information, Lifetime of the SA, Mode: Transport or tunnel or wildcard, and Path MTU

Simple inbound and outbound SAs



Security Policy Database (SPD)

- SPD specifies what security services are to be applied to IP packets and how.
- It discriminates between traffic that is to be IPSec-protected & traffic allowed to bypass IPSec.
- SPD maps IP traffic to specific SAs
  - Match subset of IP traffic to relevant SA
  - Use selectors to filter outgoing traffic in order to map it to a particular SA. Determine the SA if any for this packet and its associated SPI
  - Based on SPD entries (local & remote IP addresses, next layer protocol, name, local & remote ports, action), do the required IPsec processing (AH or ESP)

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

Transport Mode vs. Tunnel Mode

IP payload is encrypted

IP header is not encrypted

Original IP header is used for routing

Does not protect IP header, only protects the information coming from the transport layer

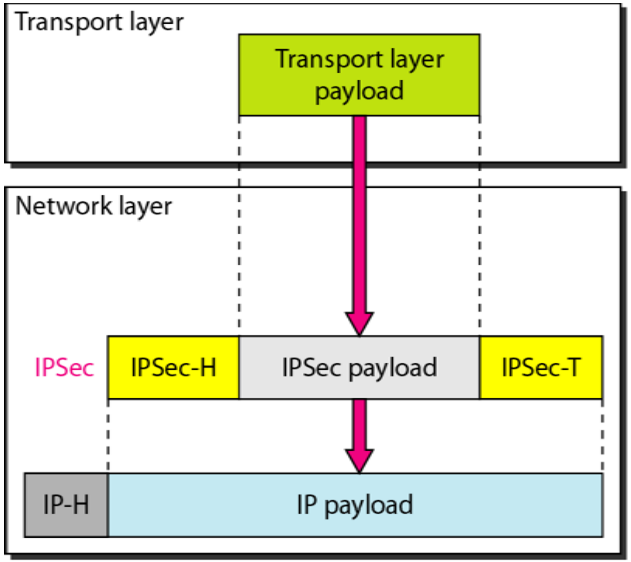
Usually used for end-to-end communication

IP payload is encrypted

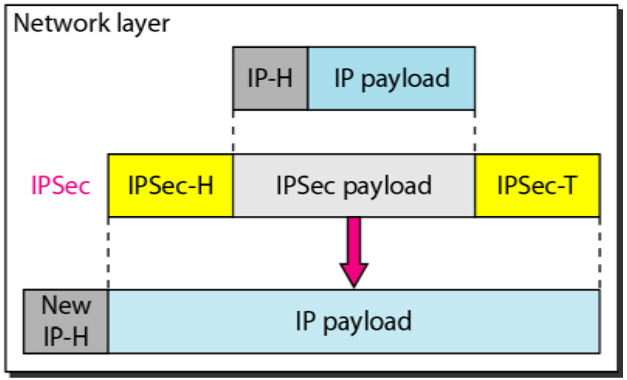
IP header is encrypted

Encapsulates original IP header into new IP header which is then used for routing

Usually used for router-to-router or firewall-to-firewall communication

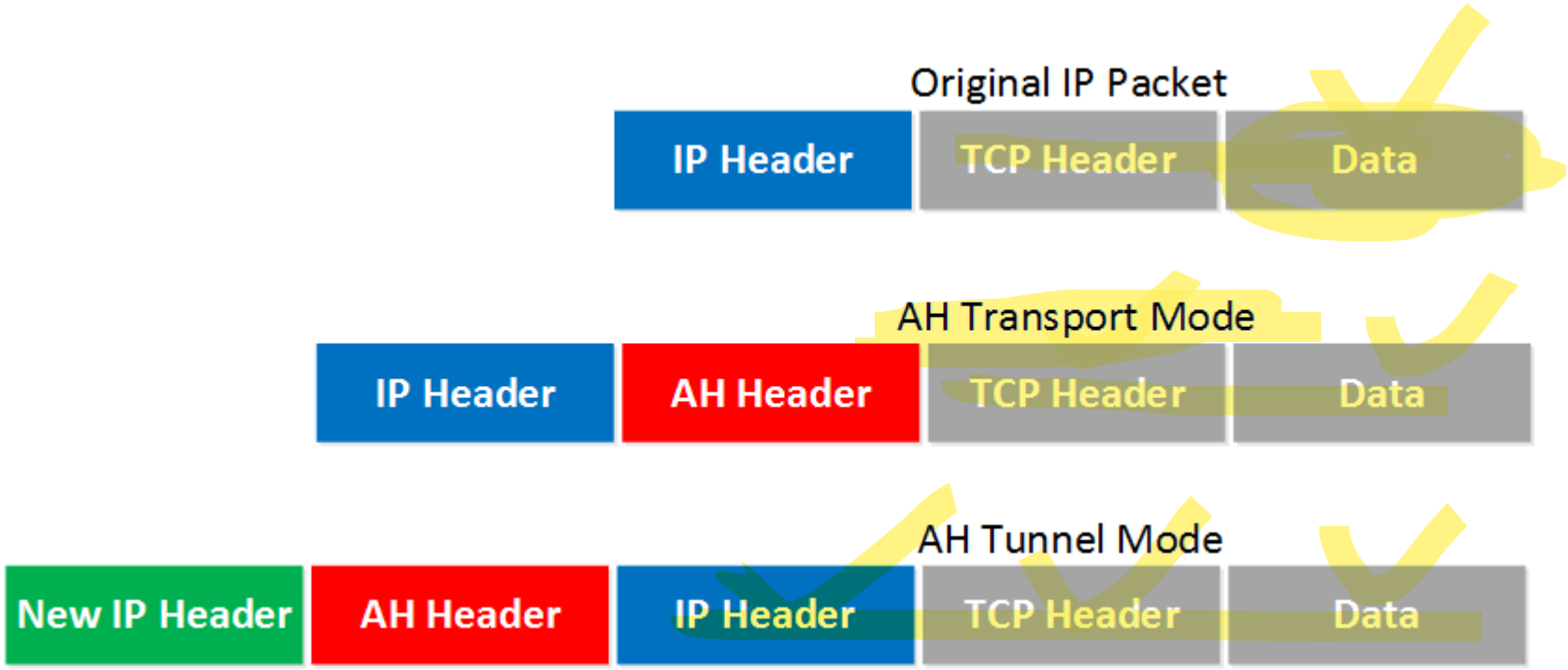


a. Transport mode



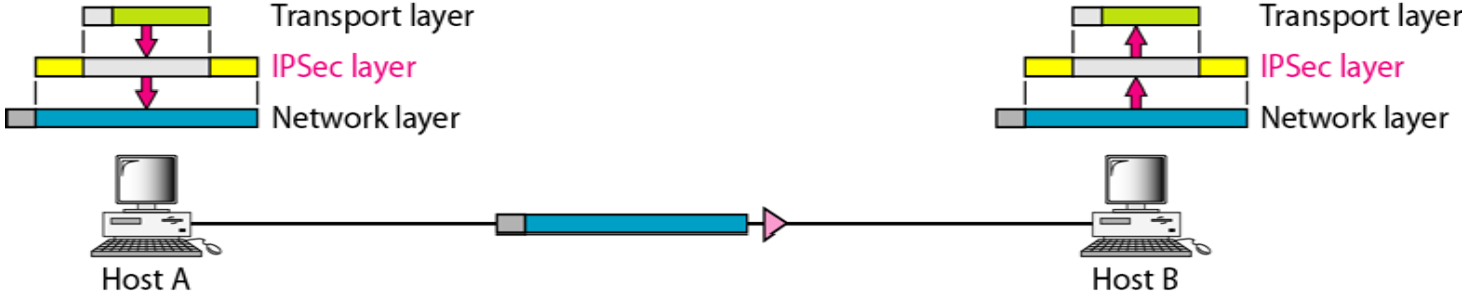
b. Tunnel mode

Transport Mode vs. Tunnel Mode

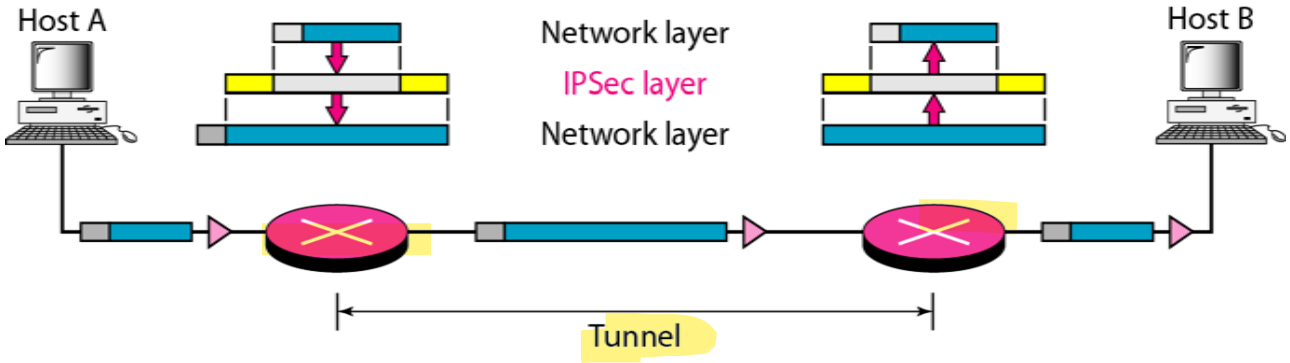


Transport and Tunnel Mode in Action

- Transport mode in action

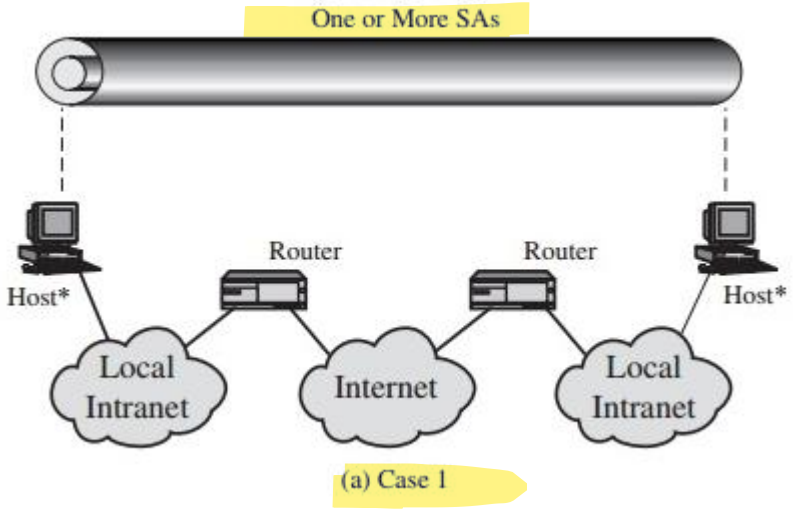


- Tunnel Mode in action



Combining Security Associations

- An SA can implement either AH or ESP, but not both
- To implement both, need to combine SAs to form a SA bundle
  - *Transport adjacency*: Outer AH over Inner ESP
  - *Iterated tunnelling*: Multiple with different end points

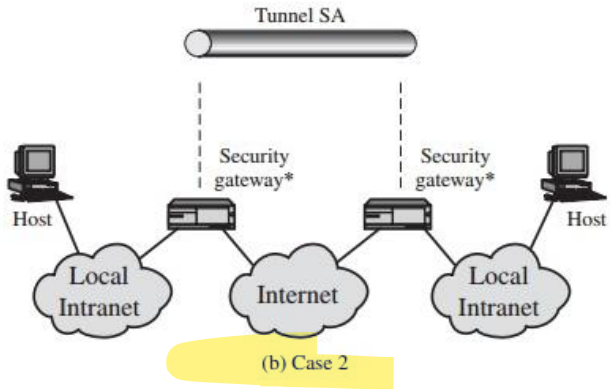


Security is provided between end systems. Among the possible combinations are:

- AH in transport mode
- ESP in transport mode
- ESP followed by AH in transport mode
- Any one of the above inside an AH or ESP in tunnel mode

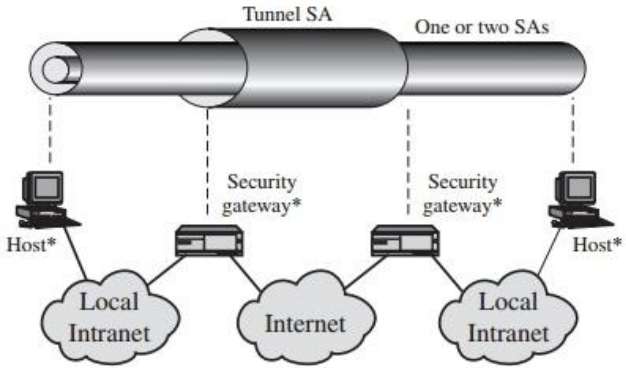
Ref: https://www.brainkart.com/article/Combining-Security-Associations_8498/

Combining Security Associations



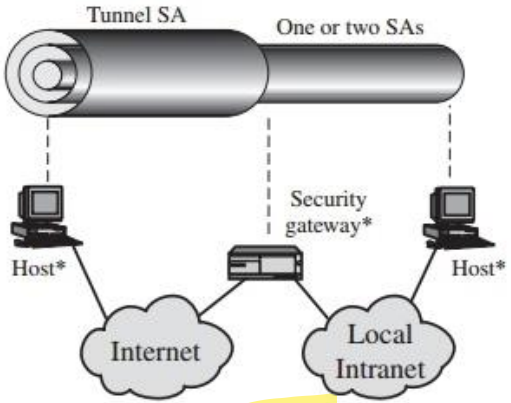
(b) Case 2

- Security is provided only between gateways.
- Only a single tunnel SA is needed for this case.
- Nested tunnels are not required.
- tunnel could support AH, ESP, or ESP with the authentication option.



(c) Case 3

- Case 2 + security at end systems also.
- Combinations for cases 1 and 2 apply here

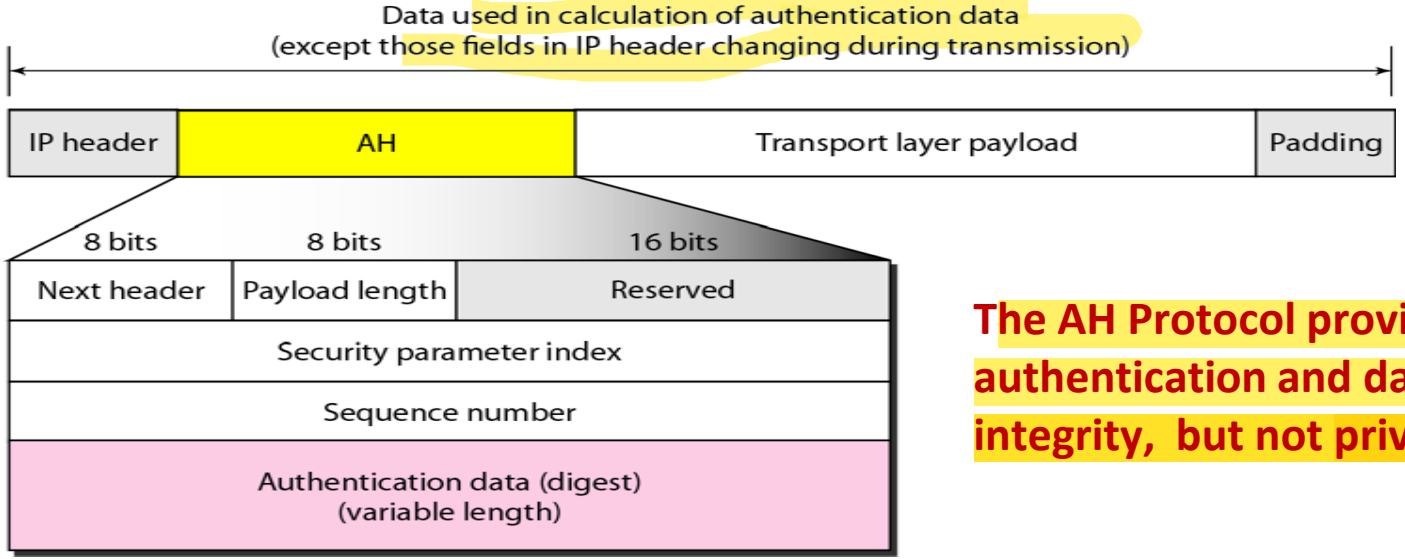


(d) Case 4

- A remote host that communicates with a workstation behind a firewall.
- Only tunnel mode is required between the remote host and the firewall.
- As in case 1, one or two SAs may be used between the remote host and the local host

Ref: https://www.brainkart.com/article/Combining-Security-Associations_8498/

IPSec Authentication Header



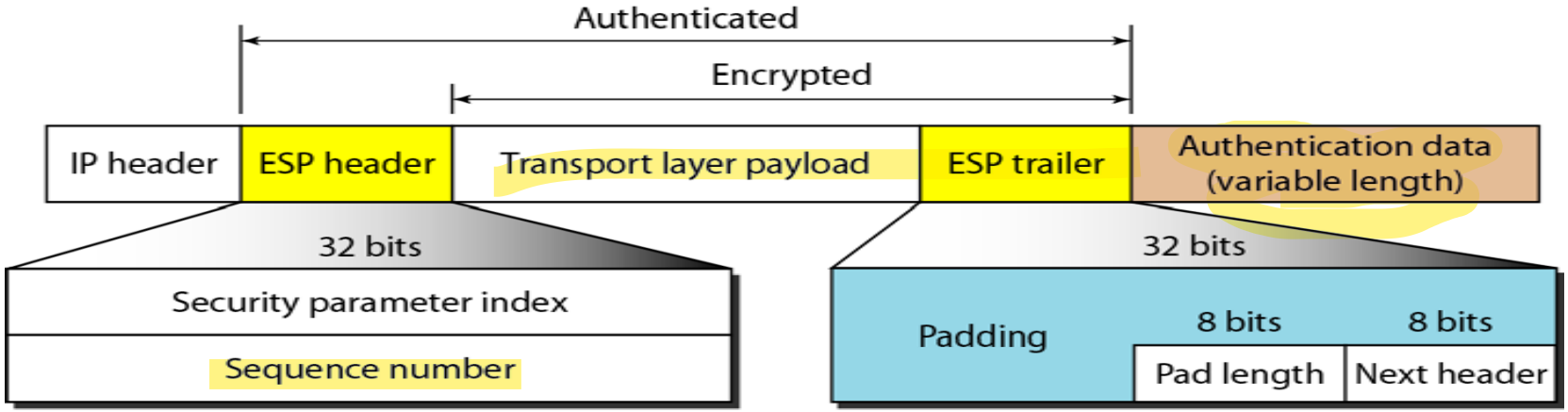
The AH Protocol provides source authentication and data integrity, but not privacy.

- **Next header** – defines the type of payload carried by the IP datagram (such as TCP, ICMP, UDP)
- **Payload length** – defines the length of the Authentication Header
- **Security Parameter Index** – helps the receiver know which connection this packet belongs to
- **Sequence Number** – provides ordering information; helps against replay attacks
- **Authentication Data** – A variable length field that contains Integrity Check Value (ICV) for the packet

AH ICV calculation

- The AH ICV is computed over:
  - IP header fields that are either immutable in transit or that are predictable in value upon arrival at the endpoint, e.g., source address (immutable), destination address with source routing (mutable but predictable)
  - The AH header (Next Header, Payload Len, Reserved, SPI, Sequence Number, and the Authentication Data (which is set to zero for this computation), and explicit padding bytes (if any))
  - The upper level protocol data, which is assumed to be immutable in transit

IPSec Encapsulating Security Payload Header



ESP provides source authentication, data integrity, and privacy.

ESP

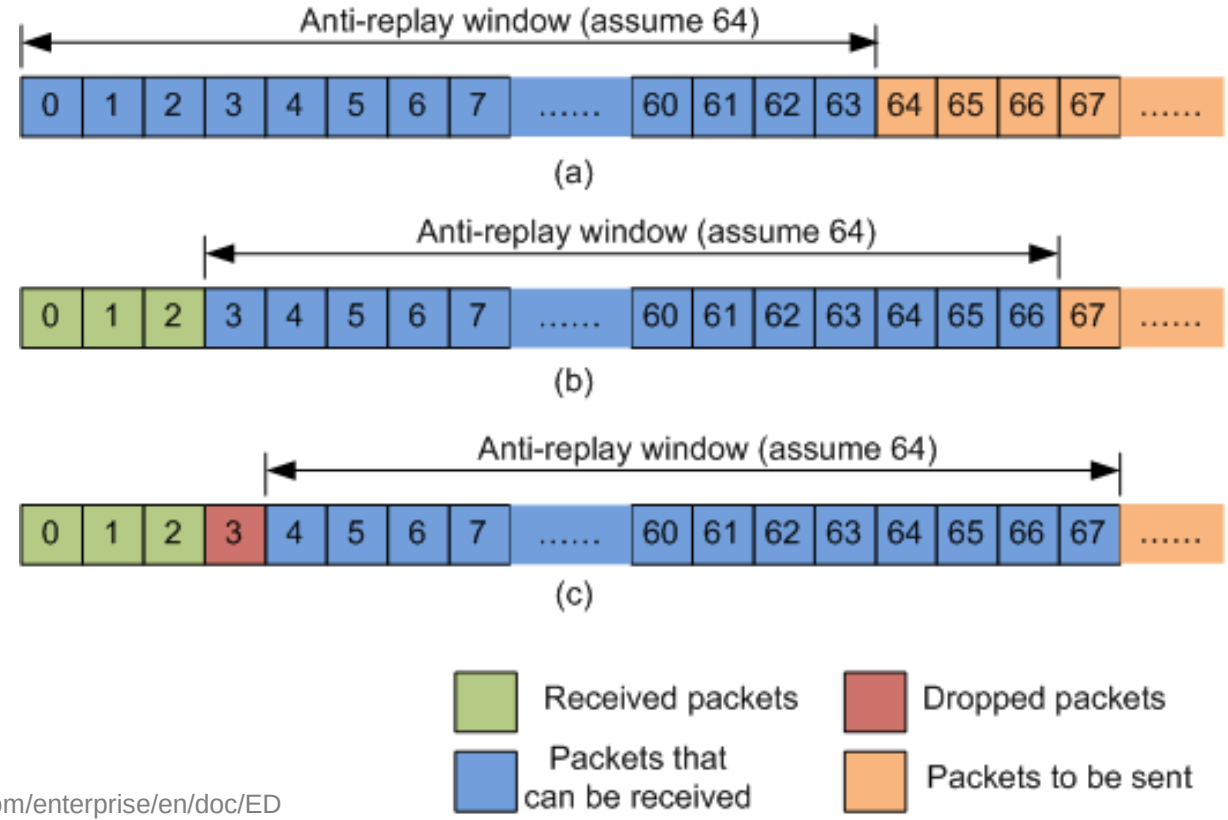
- ESP Provides:
  - Message content confidentiality,
  - Data origin authentication,
  - Connectionless integrity,
  - Anti-replay service,
  - Limited traffic flow confidentiality
  - Services depend on options selected when establish Security Association (SA), net location
  - Can use a variety of encryption & authentication algorithms

Anti-Replay Service

- In replay attacks, attackers send a large number of packets that have already been received by destination hosts.
- IPsec implements anti-replay using the sequence number and sliding window. When an IPsec SA is negotiated by both entities, the Sequence Number field is initialized to 0, and is increased by 1 each time the sender sends a packet.
- An anti-replay sliding window and a database storing sequence numbers of the received packets are configured for the receiver.
  - If a packet with a sequence number is not received before and the sequence number is within the anti-replay window, the receiver accepts the packet. If the packet with the sequence number has been received, the receiver considers that it is a replay attack packet and discards it.
  - If the sequence number is on the left of the anti-replay window (the sequence number is less than the minimum value of the anti-replay window), the receiver considers that the packet has been received and discards it.
  - If the sequence number is on the right of the anti-replay window (the sequence number is larger than the minimum value of the anti-replay window), the receiver considers that the packet is not received, accepts it normally, and moves the anti-replay window to the right.

Ref: https://support.huawei.com/enterprise/en/doc/EDOC1100059464/7cb31f38/ipsec-security

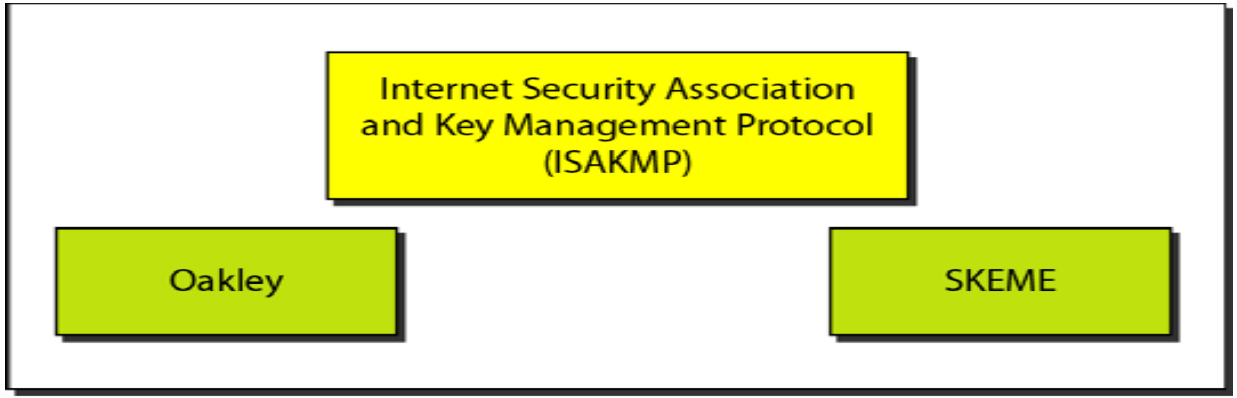
Anti-Replay Service



Ref:
https://support.huawei.com/enterprise/en/doc/EDOC1100059464/7cb31f38/ipsec-security

Internet Key Exchange (IKE)

- Handles key generation & distribution
- Typically need 2 pairs of keys - 2 per direction for integrity and confidentiality
- Manual key management - system admin manually configures every system
- Automated key management - automated system for on demand creation of keys for SA's in large systems



Internet Key Exchange (IKE)

IKE creates SAs for IPSec

Internet Key Exchange (IKE)

- IKE is a hybrid protocol based on:
  - ***ISAKMP***:
    - Internet Security Association and Key Management Protocols are used to establish, negotiate, modify, and delete SAs.
    - Provides framework for key management
    - This protocol establishes a secure connection between two IPSec peers.
    - It is independent of key exchange protocol, encryption algorithm, and authentication method.
  - ***Oakley***: Oakley defines the mechanism that is used for key exchange over an IKE session. The default algorithm for key exchange used by this protocol is the Diffie-Hellman algorithm.
  - ***SKEME***: This protocol is another version for key exchange

Oakley

- A key determination protocol based on D-H key exchange
- Adds features to address weaknesses of D-H.
- D-H has no info on identities of parties, is subject to man-in-middle attack, is computationally expensive
- Oakley adds
  - Cookies to thwart DoS attacks
  - Several groups of pre-specified global parameters
  - Nonces to protect against replay
  - DH public key exchange with authentication using Digital signature, Public Key Encryption, or Symmetric Key Encryption
- Can use arithmetic in prime fields or elliptic curve fields

IPSec Conclusion

- IPSec provides authentication, confidentiality, and key management at Layer 3. Applies to all traffic.
- Security associations are one-way and can be bundled together.
- Authentication header for message authentication using HMAC
- Encapsulating security protocol (ESP) for confidentiality and/or integrity
- Both can be used end-to-end with original IP header inside (Tunnel) or without original IP header (Transport) mode
- Oakley is the IKE key determination protocol
- ISAKMP is the IKE key management protocol

References

- http://www.cse.wustl.edu/~jain/cse571-17
- Forouzan, B. A., COOMBS, C., & FEGAN, S. C. (1998). Data communications and networking. Language, 32(908), 23cm.
- Internet security http://www.cis.syr.edu/~wedu/Teaching/cis758/readings.html
- Open Learn https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=48261
- IDPS https://cloudacademy.com/course/intrusion-detection-and-prevention-on-amazon-web-services/ids-ips-in-detail-1/
- G. Dileep Kumar, "Network Security Attacks and Countermeasures", IGI Global, 2016.