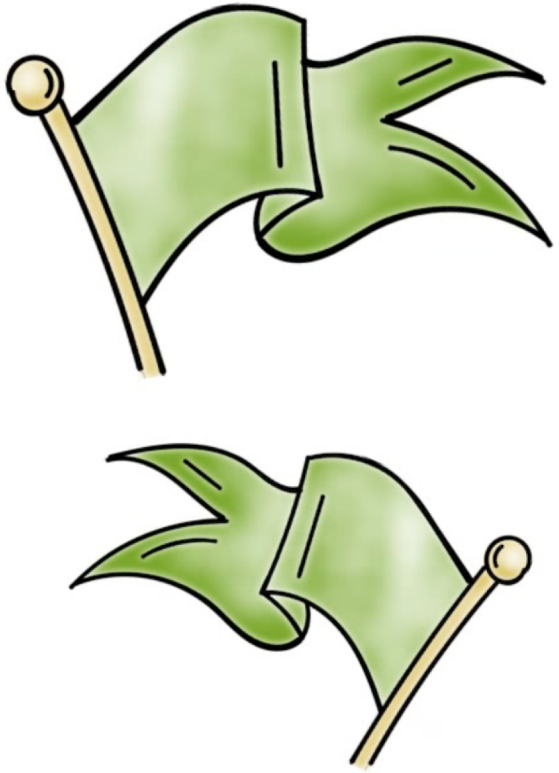
IPSec and TLS
Lesson Introduction

- IPSec and the Internet key exchange protocol
- Transport layer security protocol

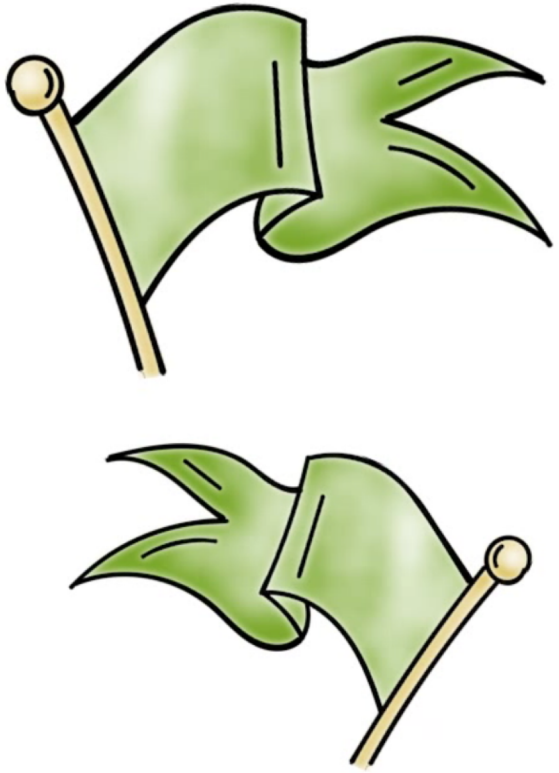
Goals of IPSec



IP spoofing is a common technique in cyber attacks

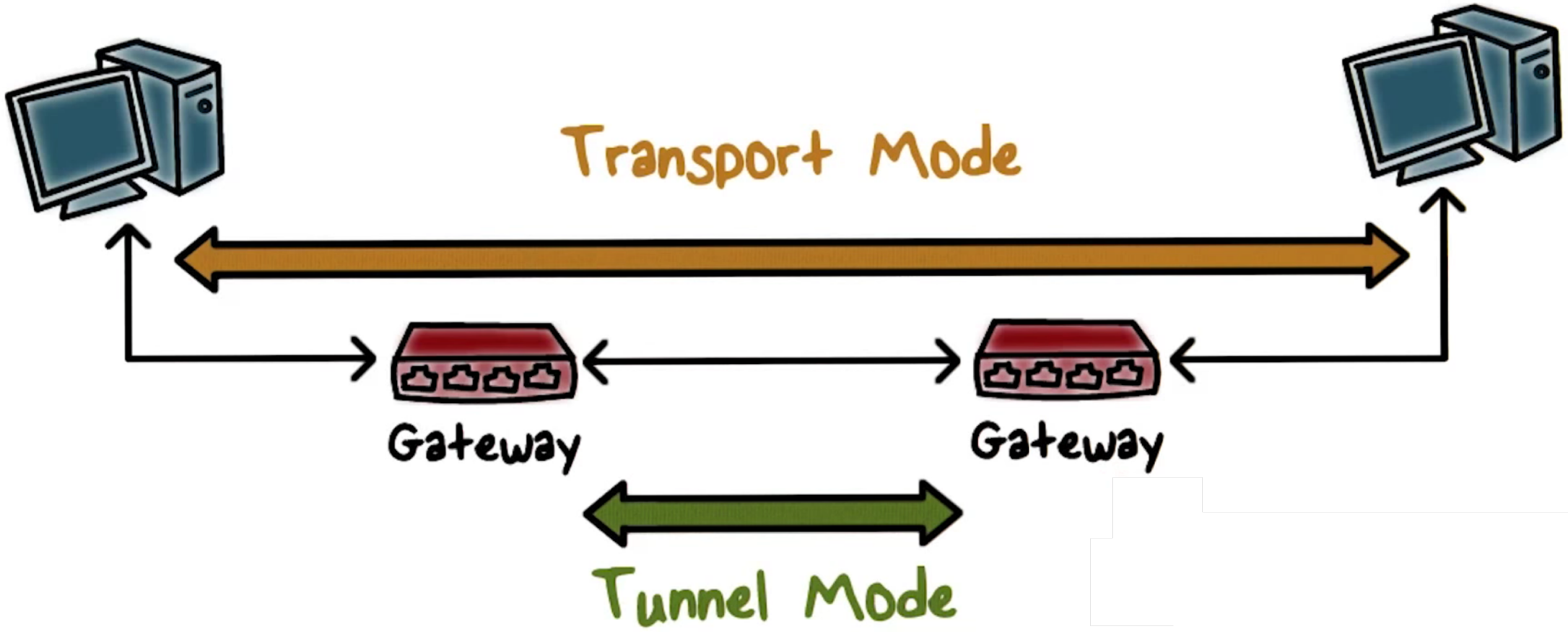
- Bots spoof the an IP address of a victim web site
- Then send DNS queries to DNS servers
- The DNS servers respond, sending large amounts of data to the victim
- **Result: a denial-of-service attack**

Goals of IPSec

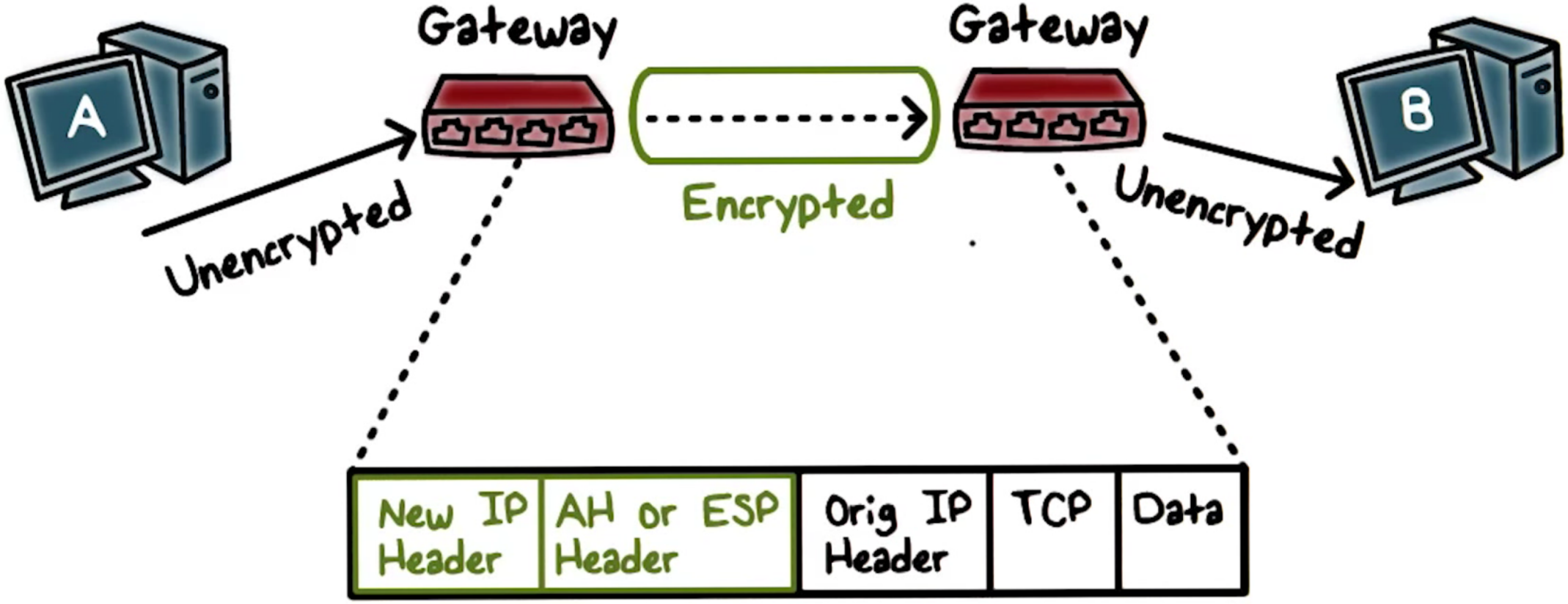


- **Verify sources of IP packets**
  - Provide **Authentication** that is lacking in IPv4
- Protect integrity and/or confidentiality of packets
- Prevent replaying of old packets
- **Provide security automatically** for upper layer protocols and applications

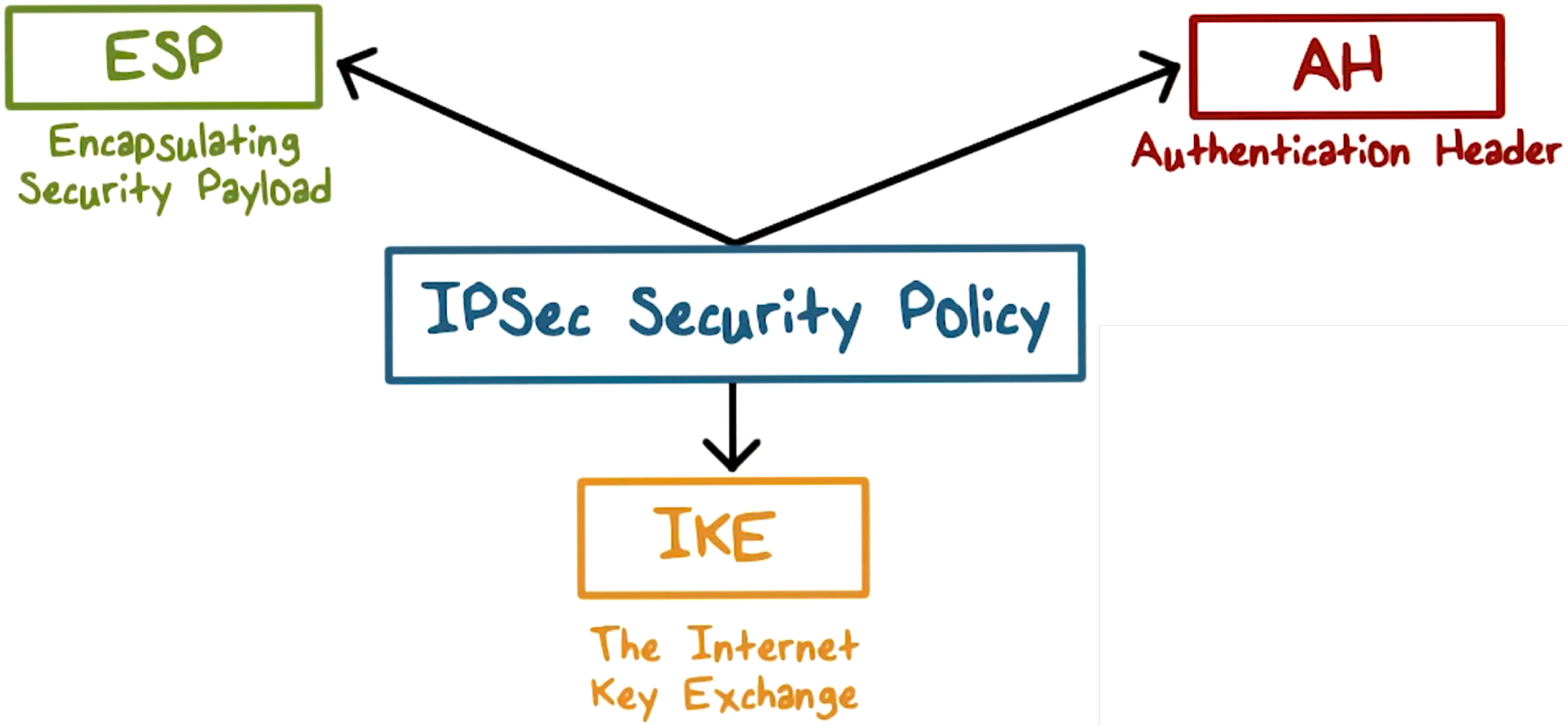
IPSec Modes



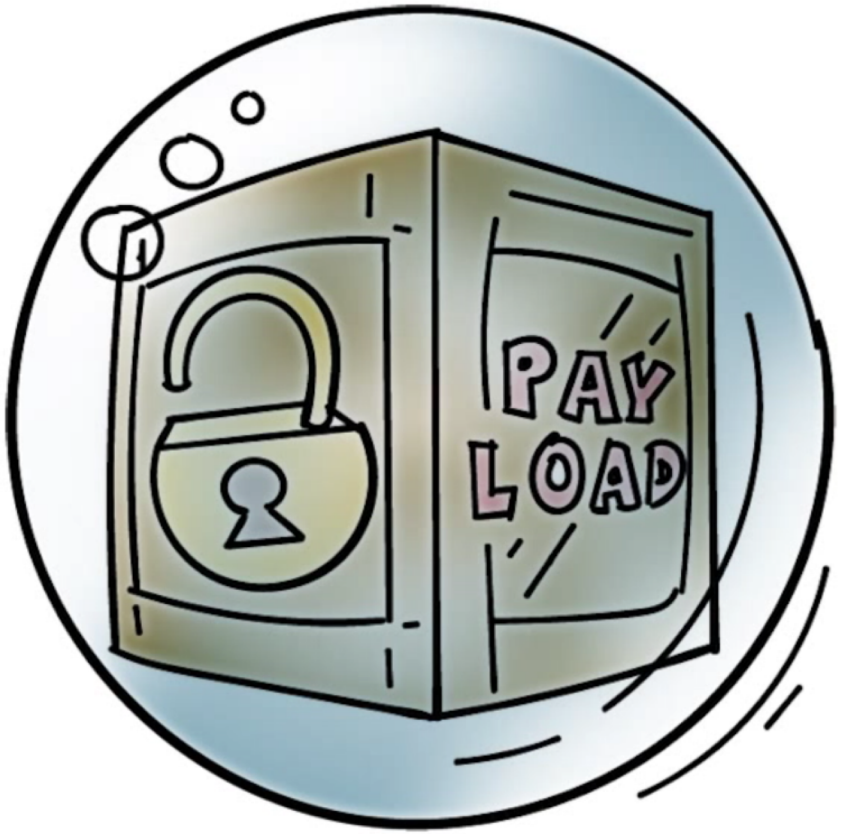
Tunnel Mode


A
Gateway
Gateway
B
Unencrypted
Encrypted
Unencrypted
New IP Header
AH or ESP Header
Orig IP Header
TCP
Data

IPSec Architecture

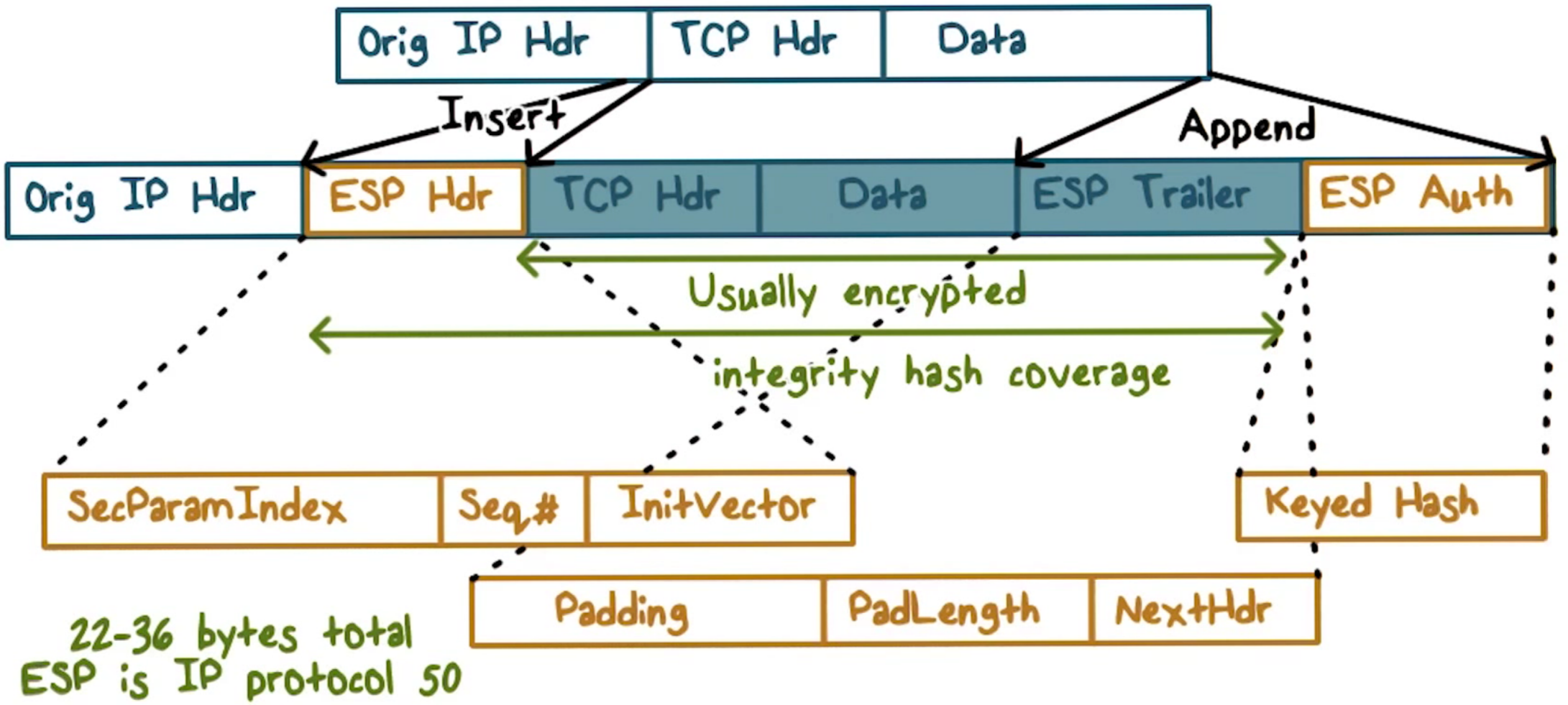


Encapsulated Security Payload (ESP)

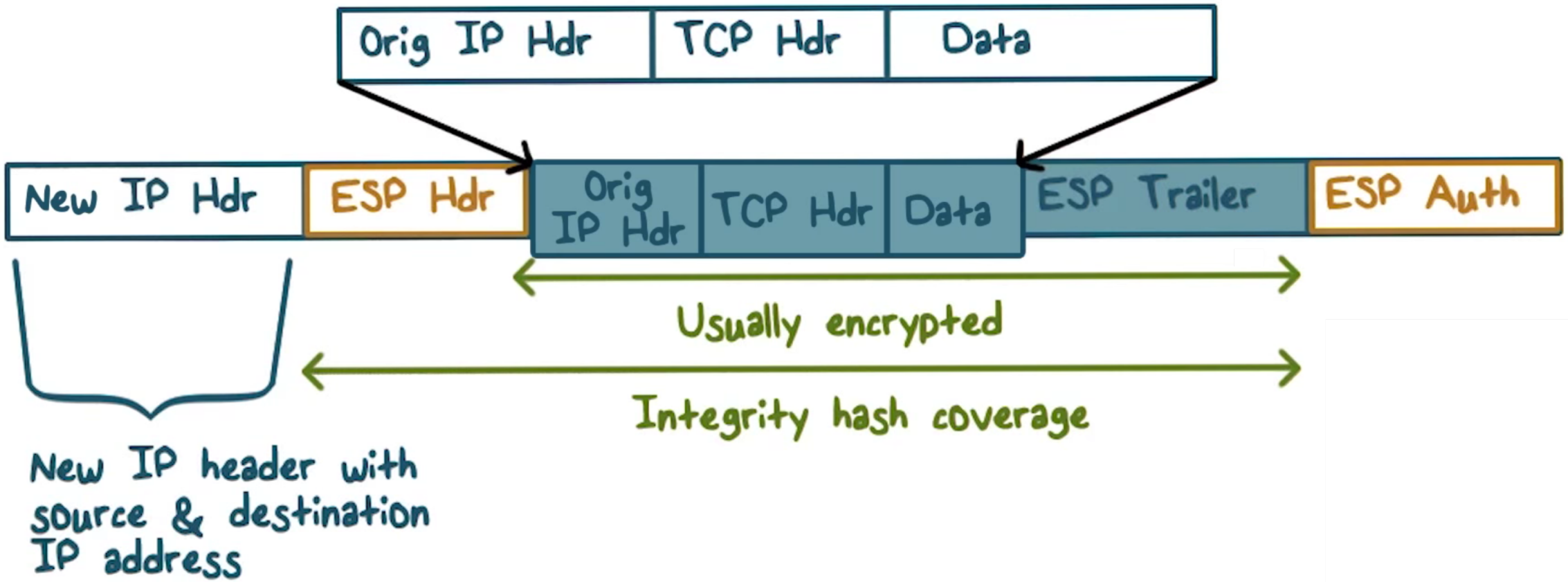


- Encrypt and authenticate each packet
- **Encryption is applied to packet payload**
  not applied to the header
- Authentication is applied to data in the **IPSec header as well as the data contained as payload**, after encryption is applied

ESP in Transport Mode



ESP Tunnel Mode

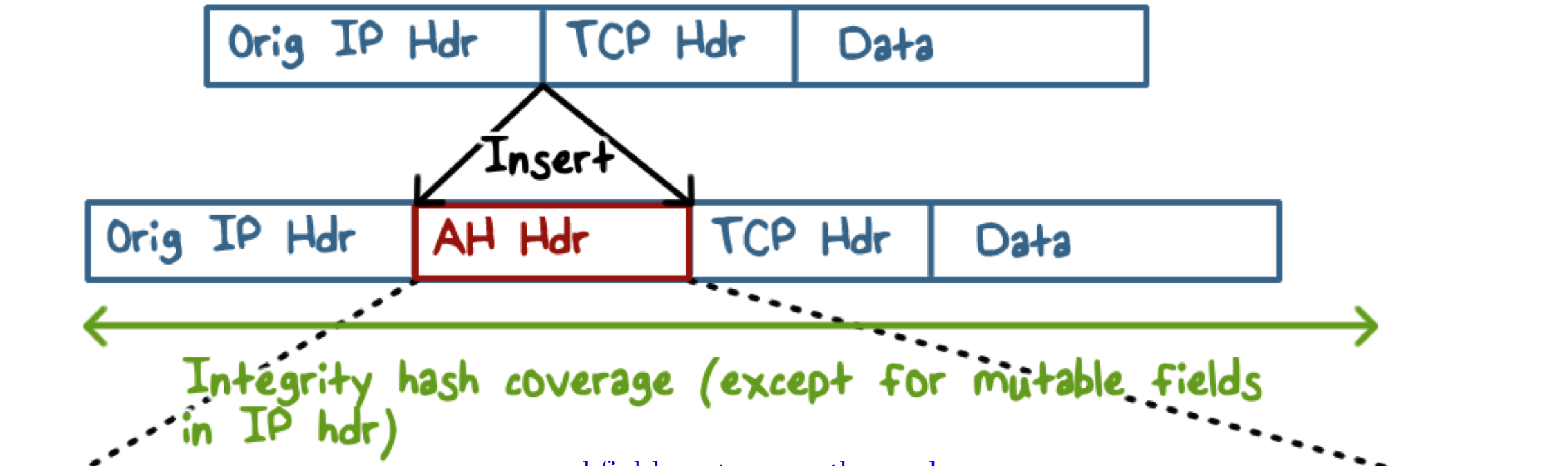


Authentication Header (AH)

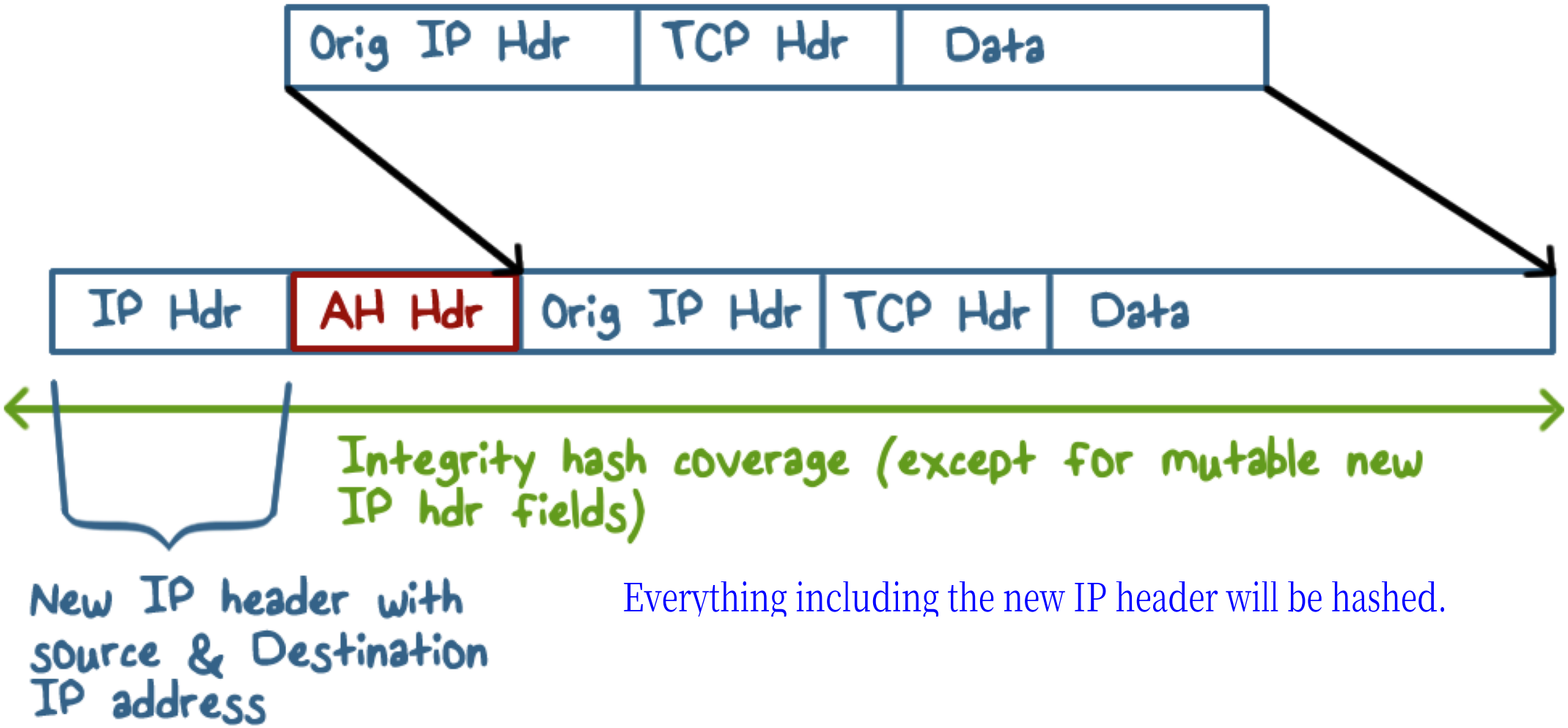
- Authentication is applied to the entire packet, with the **mutable fields in the IP header "zeroed out"**

- If both ESP and AH are applied to a packet, **AH follows ESP**

Authentication Header in Transport Mode



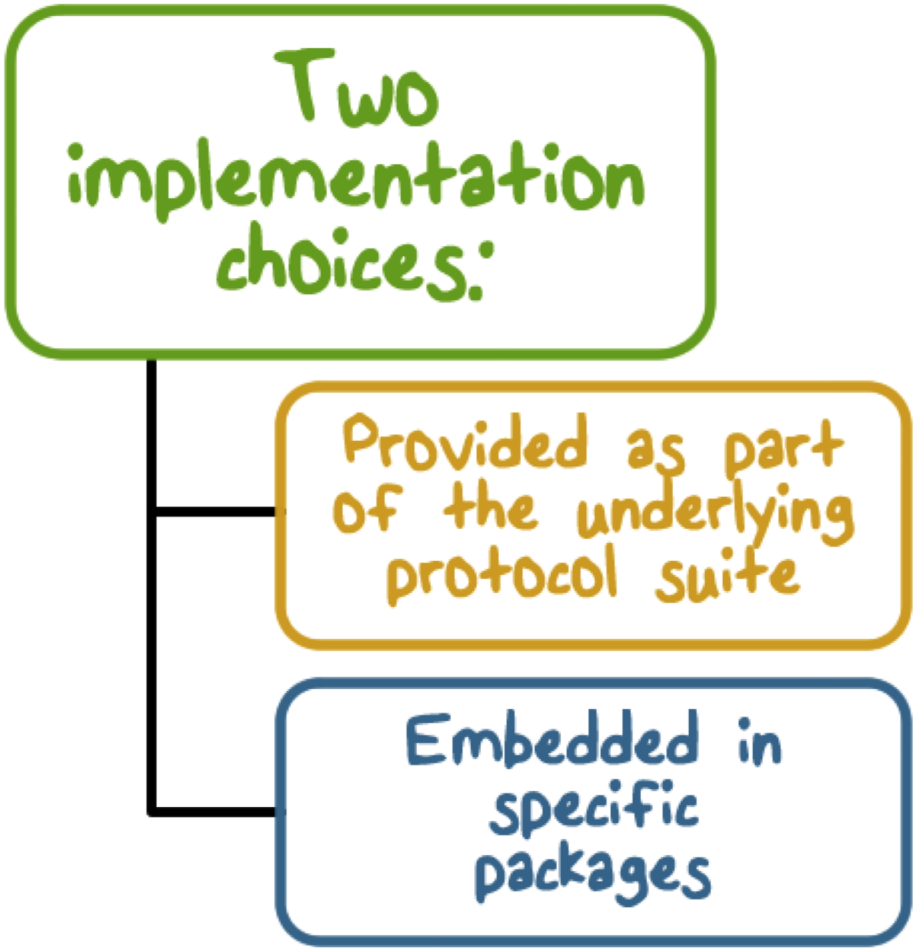
Authentication Header in Tunnel Mode



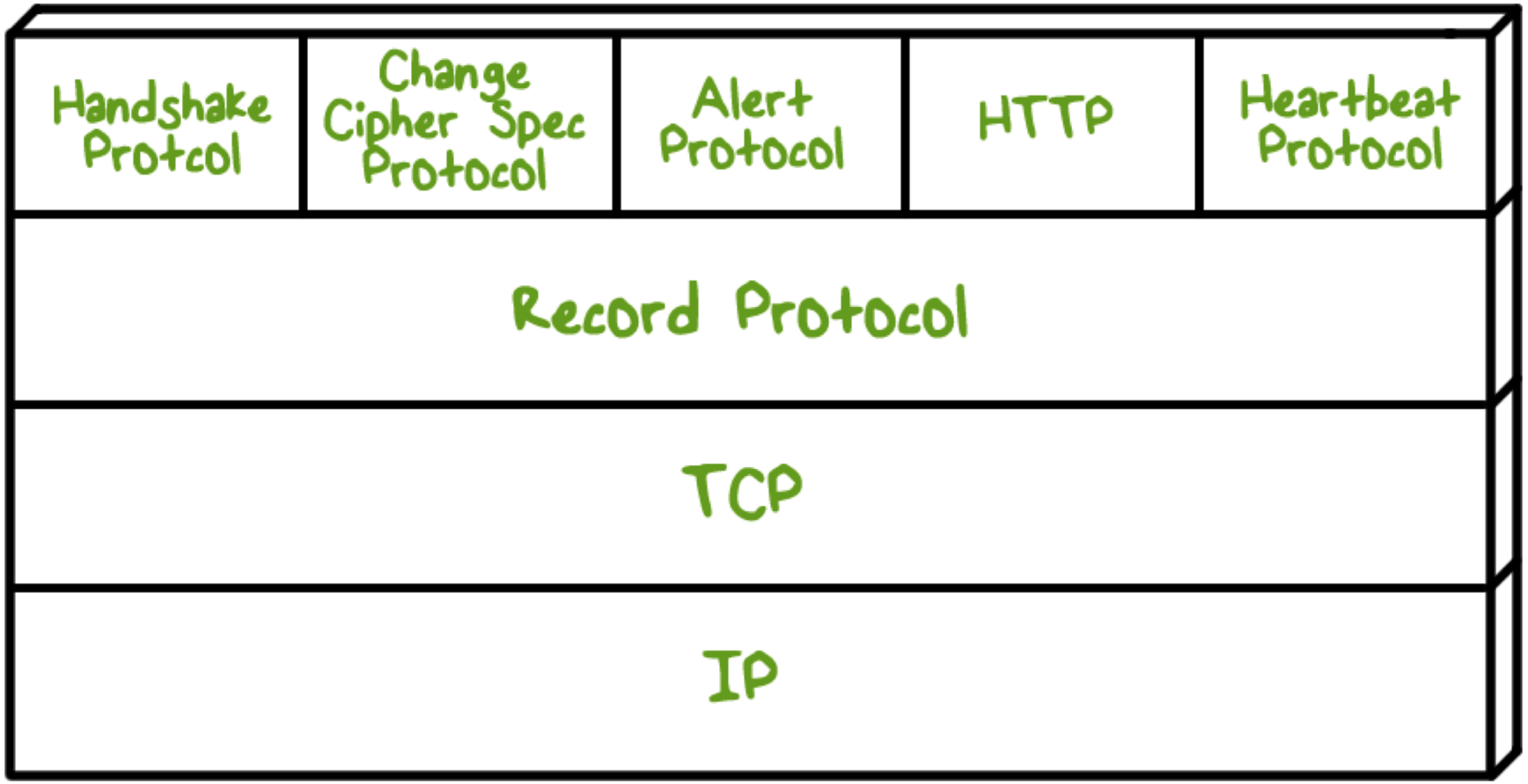
Everything including the new IP header will be hashed.

Secure Socket Layer (SSL) and Transport Layer Security (TLS)

- One of the most widely used security services
- General-purpose service implemented as a set of protocols that rely on TCP
- Subsequently became Internet standard: Transport Layer Security (TLS)



Secure Socket Layer (SSL) and Transport Layer Security (TLS)



TLS Concepts

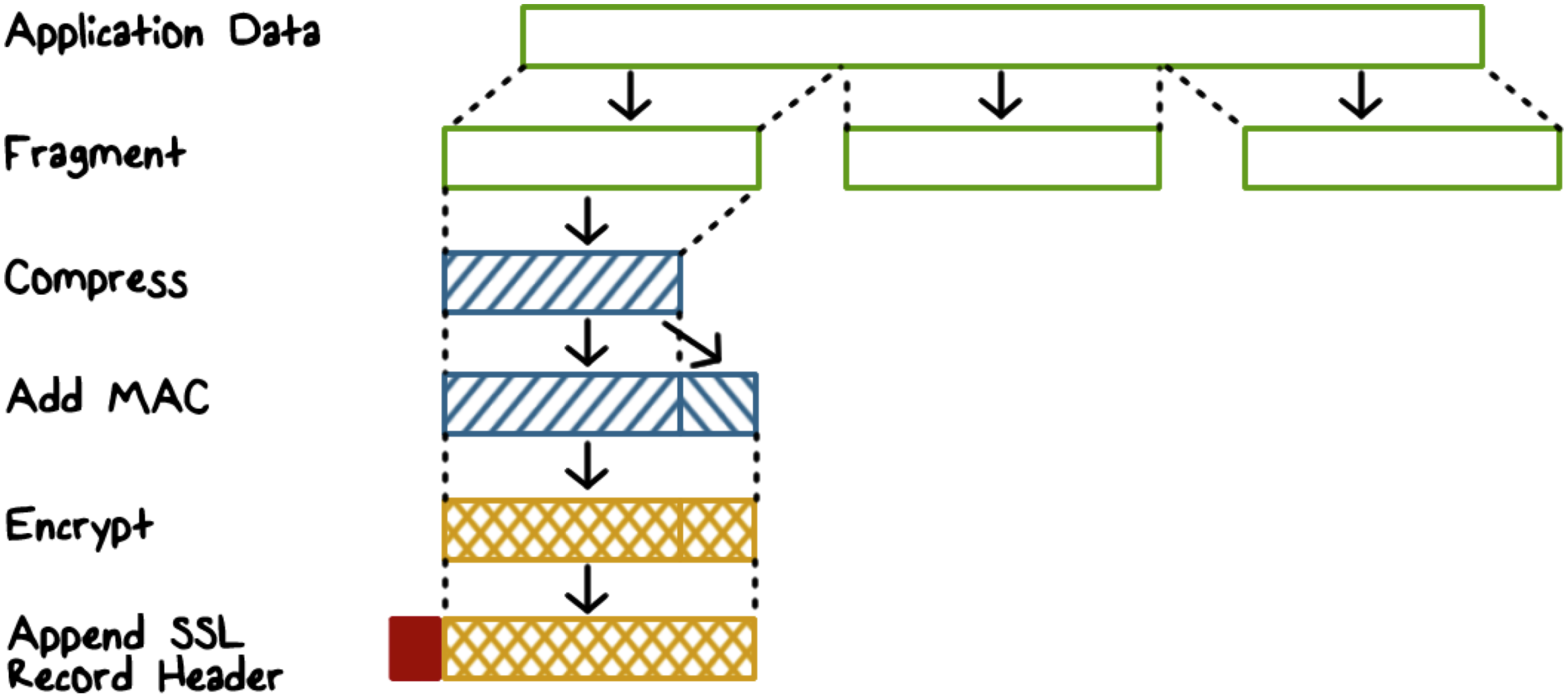
TLS Session

- An association between a client and a server
- Created by the Handshake Protocol
- Define a set of cryptographic security parameters
- Used to avoid the expensive negotiation of new security parameters for each connection

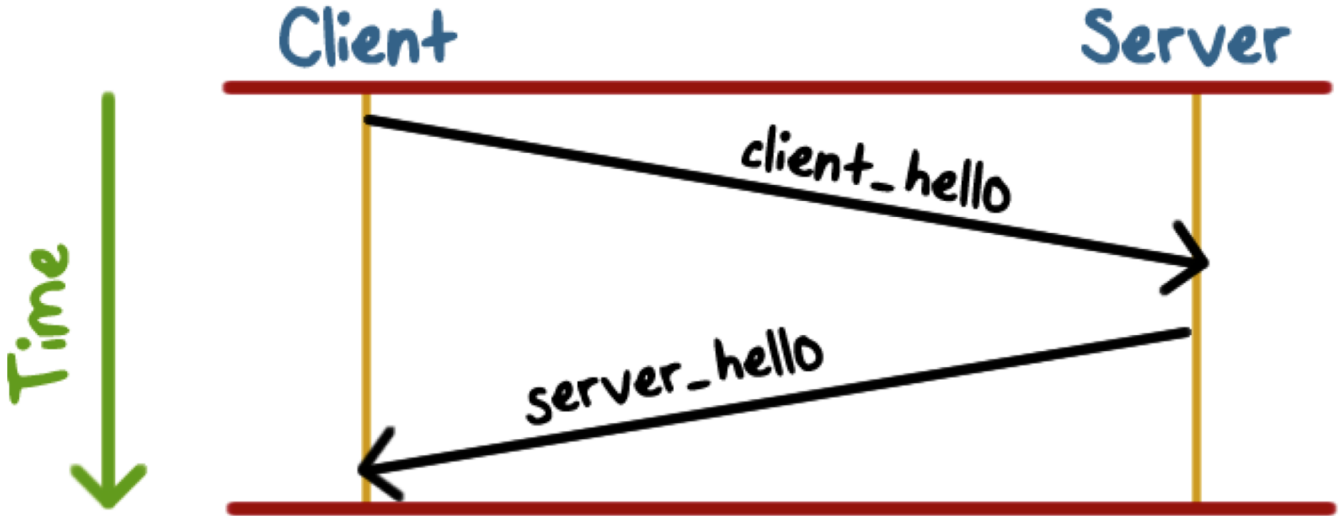
TLS Connection

- A transport (in the OSI layering model definition) that provides a suitable type of service
- Peer-to-peer relationships
- Transient
- Every connection is associated with one session

SSL Record Protocol



The Handshake Protocol



Phase 1

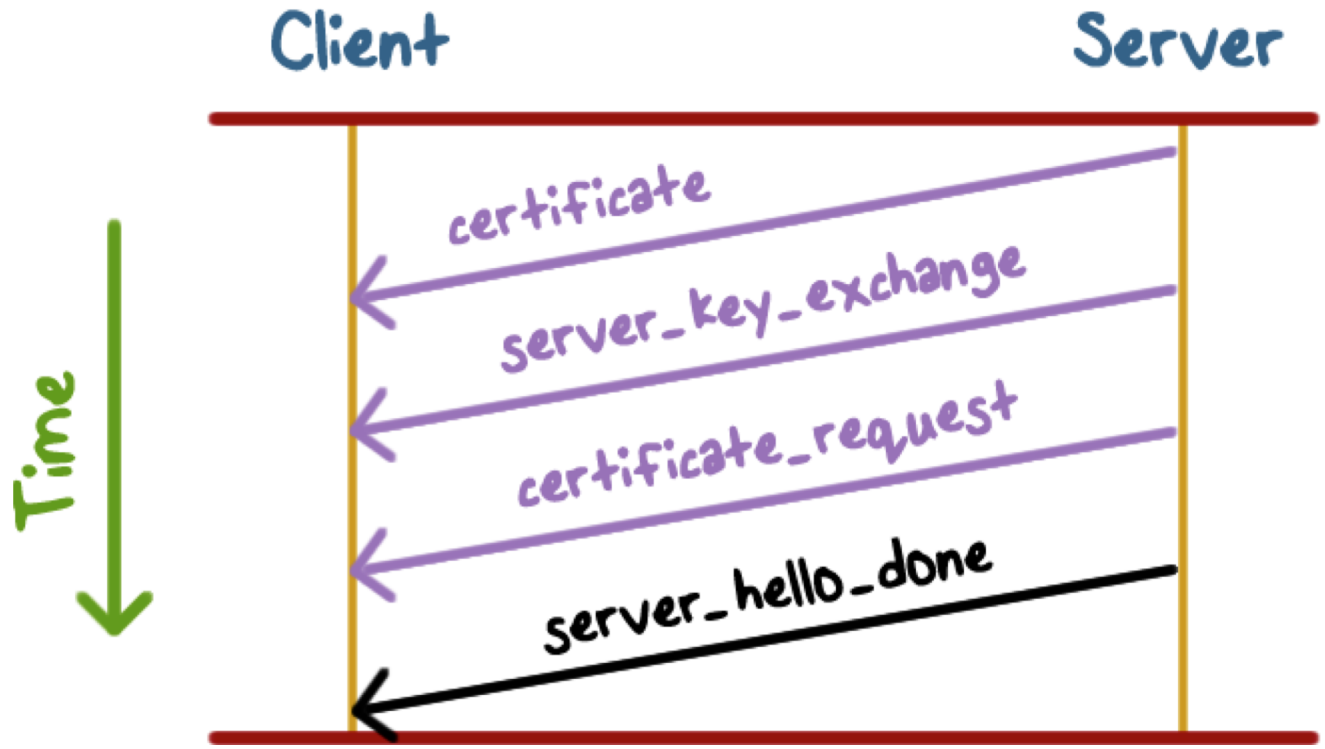
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

The Handshake Protocol

The Parameters:

- **Version:** the highest TLS version understood by the client
- **Random:** a 32-bit timestamp and 28 bytes generated by a secure random number generator
- **Session ID:** a variable-length session identifier
- **CipherSuite:** a list containing the combinations of cryptographic algorithms supported by the client
- **Compression Method:** a list of compression methods supported by the client

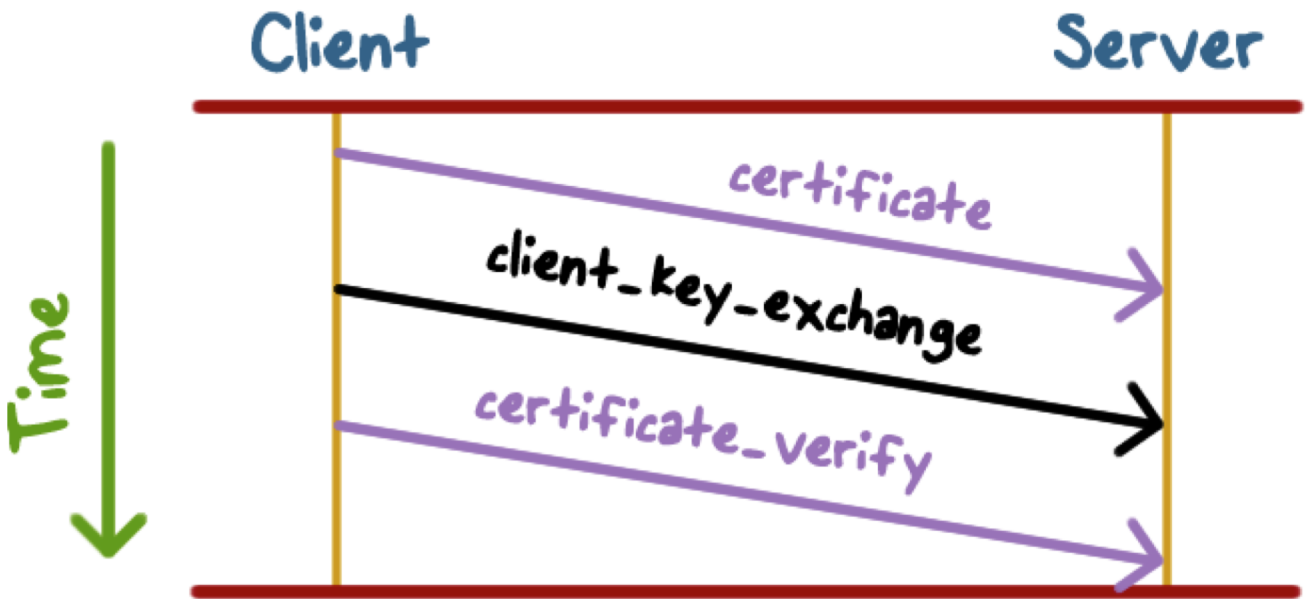
The Handshake Protocol



Phase 2

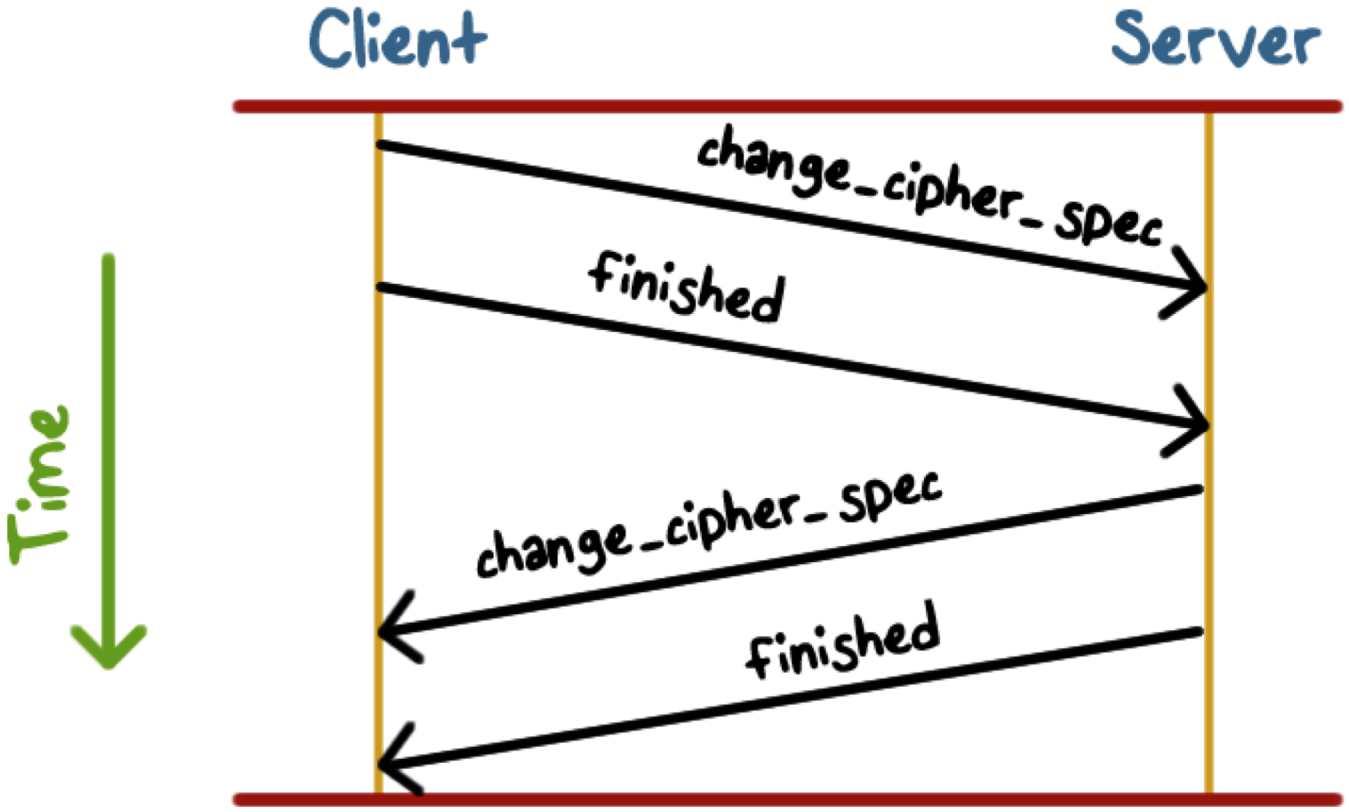
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

The Handshake Protocol



Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

The Handshake Protocol



Phase 4
Change cipher suite and finish handshake protocol.

IPSec and TLS

Lesson Summary

- IPSec can operate in tunnel or transport mode
- Confidentiality and authenticity protection provided through ESP and AH
- The one-way security association stores security parameters.
- SSL/TLS has two layers: record protocol, and handshake, change cipher spec and alert protocols