IP-Sec

What is IP Security?

- IPSec refers to a collection of communication rules or protocols used to establish secure network connections.
- Internet Protocol(IP) is the common standard that controls how data is transmitted across the internet. IPSec enhances the protocol’s security by introducing encryption and authentication.

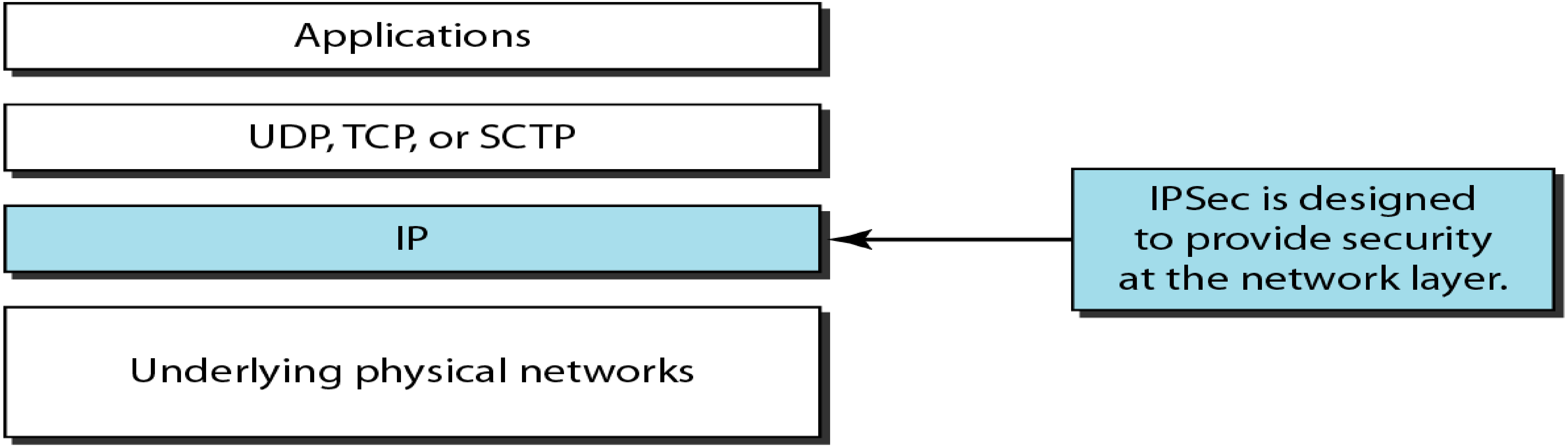
What is IPSec?

- **IPSec**
  - *stands for* **IP Security**
  - *it is used for the security of general IP traffic.*
- The power of **IPSec** lies in its ability to
  - *support multiple protocols and algorithms.*
- It also incorporates new advancements in
  - *encryption and hashing protocols.*

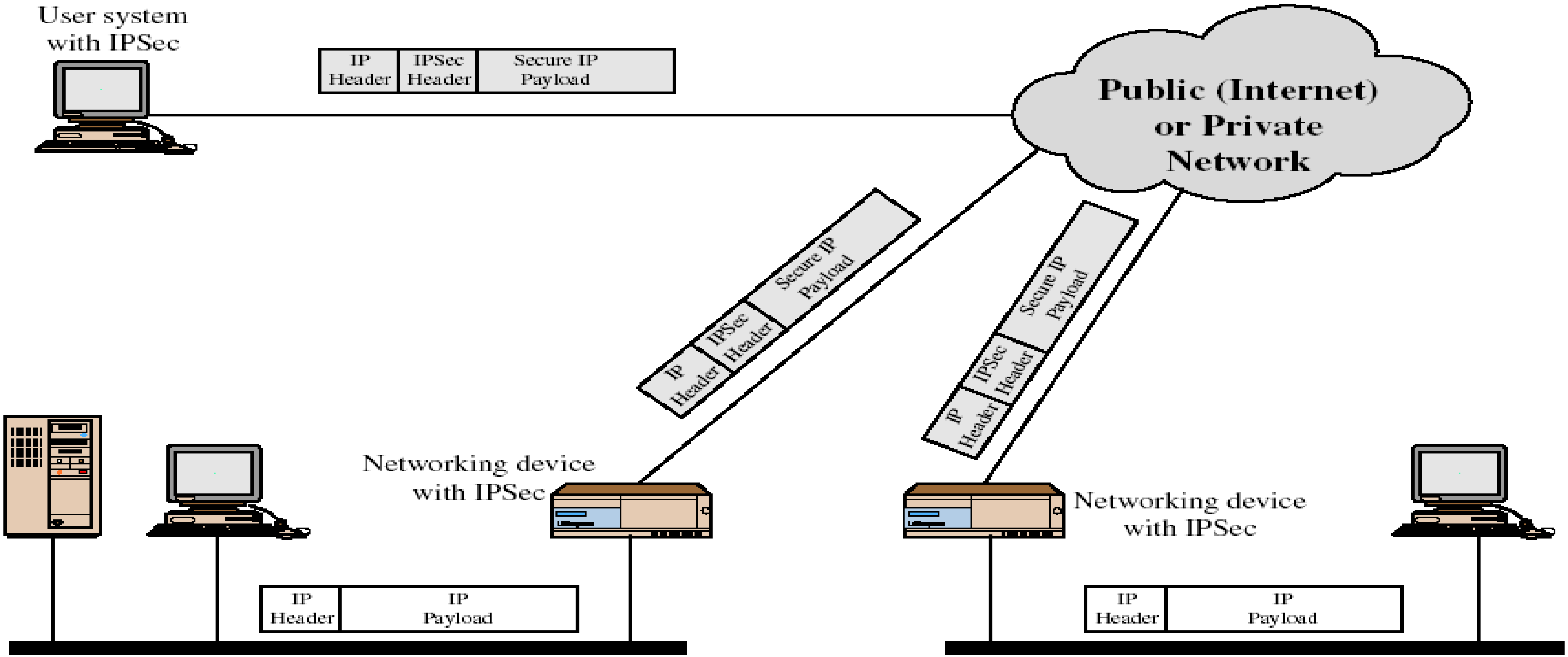
Objective of IPSec

- **Confidentiality.**
  - *IPSec uses encryption protocols namely* **AES, DES,** *and* **3DES** *for providing* ***confidentiality****.*
- **Integrity.**
  - *IPSec uses hashing protocols* **(MD5** and **SHA)** *for providing* ***integrity****. Hashed Message Authentication* **(HMAC)** *can also be used for checking the* ***data integrity****.*
- **Authentication algorithms.**
  - **RSA** *digital signatures and pre-shared keys* **(PSK)** *are two methods used for* ***authentication*** *purposes.*

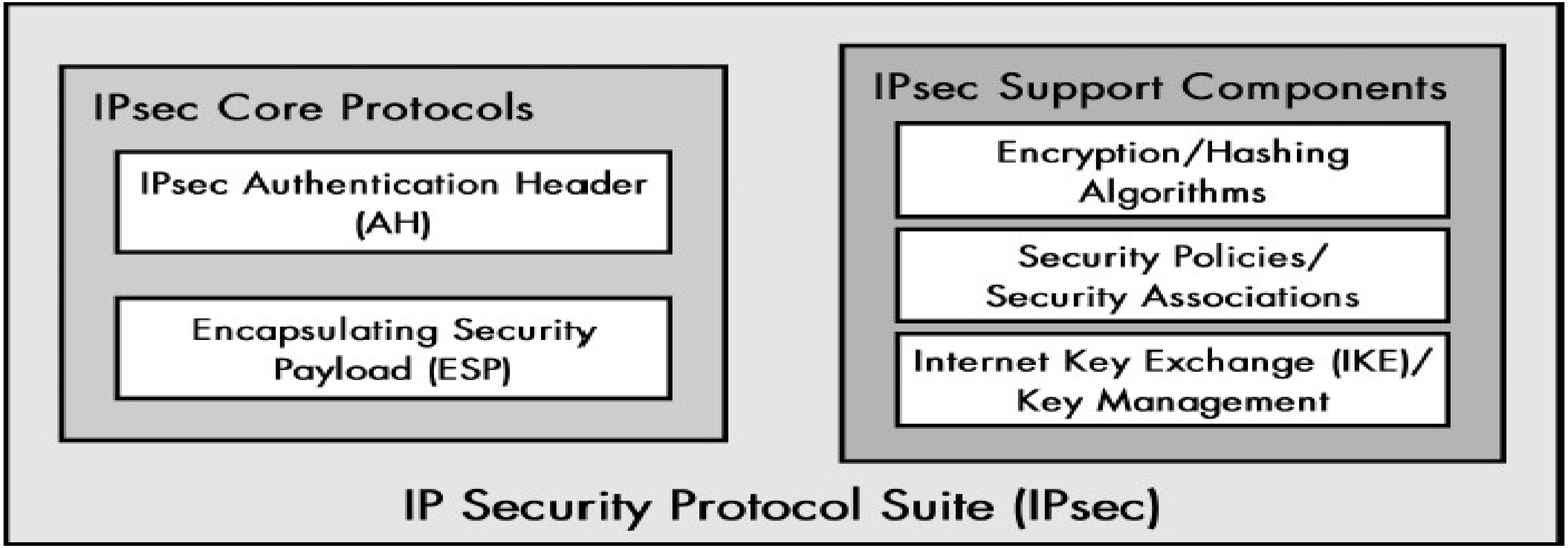
TCP/IP protocol suite and IPSec


Applications
UDP, TCP, or SCTP
IP
Underlying physical networks
IPSec is designed to provide security at the network layer.

IP security scenario



IPSec



IPsec Core Protocols

IPsec Authentication Header (AH)

Encapsulating Security Payload (ESP)

IPsec Support Components

Encryption/Hashing Algorithms

Security Policies/ Security Associations

Internet Key Exchange (IKE)/ Key Management

IP Security Protocol Suite (IPsec)

IPSec

- **IPSec architecture:**

1.Host-host implementation:

- Putting all IPSec into all hosts devices.
- Enables end to end security between any two devices on the network.

2- Router implementation:

- Is much less work. You make changes to only a few routers instead of hundreds of clients. It provides protection only between pairs of routers.

IPSec Connection Establishment Process

- IPSec is a protocol suite used in securing communication using the Internet Protocol such that each packet communicated in the course of a particular session is authenticated and encrypted. The process of establishing an IPSec connection involves two main phases:
  - **Phase 1: Establishing the IKE (Internet Key Exchange)**
  - **Phase 2: Establishing the IPSec Tunnel**

Phase 1: Establishing the IKE (Internet Key Exchange)

- In phase 1, the main aim is to establish the secure channel the IKE tunnel, which is used to further negotiations.
- Phase 1 can operate in one of two modes:
  1. Main mode
  2. Aggressive mode

1. Main Mode

Main Mode is a six-message exchange procedure that is more secure than Aggressive Mode, although at the cost of a longer session.

- **Message Exchange**

1. **Messages 1 & 2:** Exchange of the proposed algorithms for encryption, hashing, authentication and other such parameters.
2. **Messages 3 & 4:** [The Diffie-Hellman key exchange.] The parties produce master communication keys that are secret to the two of them.
3. **Messages 5 & 6:** Verification of the participants through pre-shared keys or certificates or some other means.
4. **Outcome: From t**he IKE SA (Security Association)
   1. Several parameters are negotiated like encryption algorithms, hash algorithm
   2. Key value is exchanged using groups of Diffie-Hellman key exchange algorithm
   3. Lifetime.
5. Several values exchanged are used to derive different keys for use in IPSec connection

2. Aggressive Mode

Aggressive Mode takes less time with the exchange of three messages and is less secure since more information like identity is disclosed during the course of negotiation.

- **Message Exchange:**
- **Message 1:** The initiator transmits, its offer, its Diffie-Hellman key information and identity payload.
- **Message 2:** The responder replies with its own Diffie-Hellman information as well as an identity payload.
- **Message 3:** Sends authentication information, which is done by the initiator.
- **Outcome:** Like Main Mode, an IKE SA is created but it is done in a quicker way and it is less secure.

Phase 2: Establishing the IPSec Tunnel

Phase 2 is called Quick Mode and it aims to negotiate the IPSec Security Associations after the construction of a secure IKE between two hosts or routers

- There are two modes in Phase 2
  - Tunnel mode
  - Transport mode

Tunnel Mode

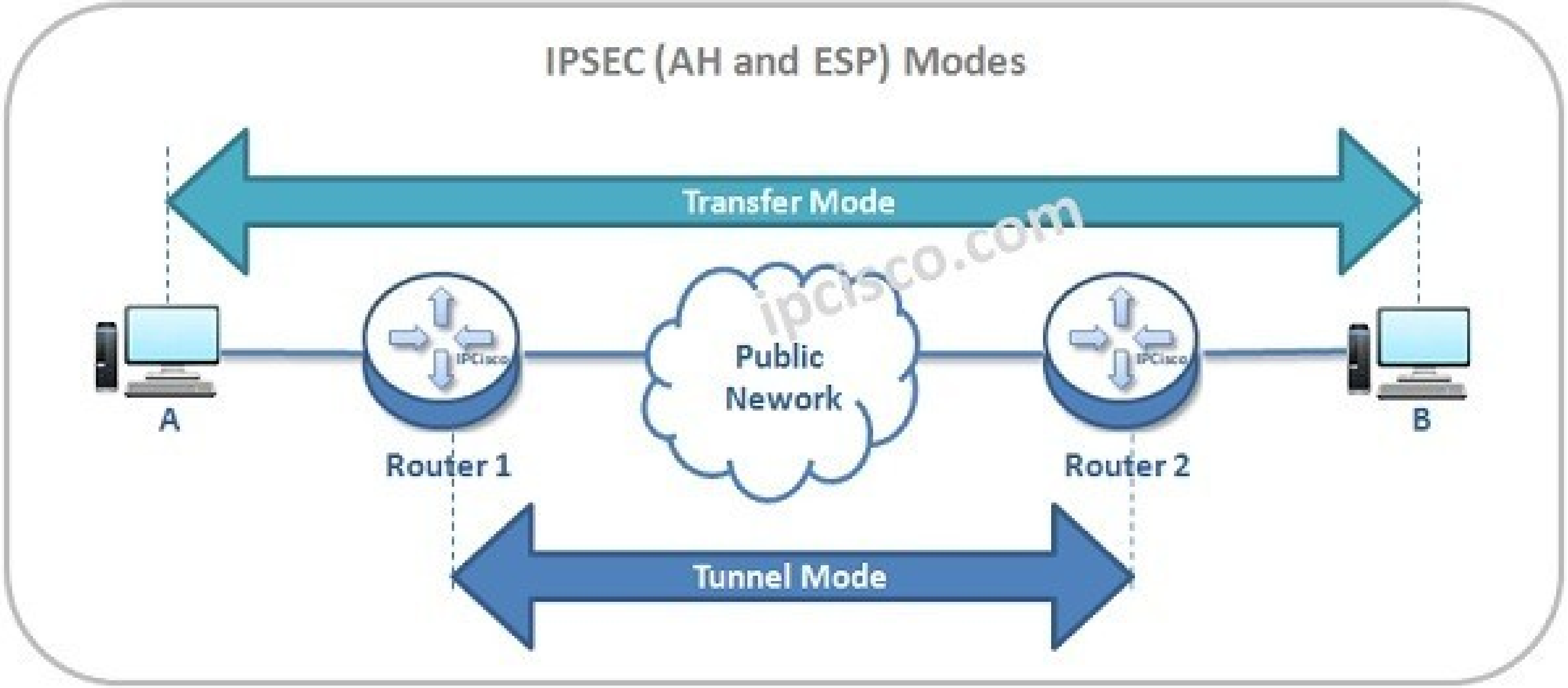
Tunnel Mode is utilized for securing communication between two networks over an intermediate network, such as the Internet.

- **Full Packet Encryption**: In this mode, the entire original IP packet, including the header and payload, is encrypted and encapsulated into a new IP packet, which includes a fresh IP header.
- **Use Case**: It is commonly used in site-to-site VPNs, connecting network gateways or routers that secure the communication between entire networks.
- **Advantages**:
  - **Protection of Internal Routing Information**: By encrypting the original packet’s IP header, tunnel mode helps obscure the routing details, which secures against traffic analysis.
  - **Gateway Compatibility**: Tunnel mode is typically mandatory for configurations where one peer acts as a security gateway for other hosts, thus ensuring enhanced compatibility across different gateway types.

Transport Mode

Transport Mode is focused on securing communication between individual hosts rather than networks.

- **Payload Encryption Only**: In this mode, only the payload of the IP packet is encrypted, while the original IP header remains intact. This is designed for end-to-end communications, such as client-to-server or host-to-host interactions.
- **Use Case**: It is suitable for applications wanting fast and secure connections, like Telnet sessions or secure file transfers.
- **Advantages**:
  - **Lower Overhead**: Since it only processes the payload, transport mode generally has less overhead compared to tunnel mode. This leads to potentially better performance.
  - **Simpler Setup**: Transport mode does not require a new IP header, making it simpler in terms of configuration and lower complexity

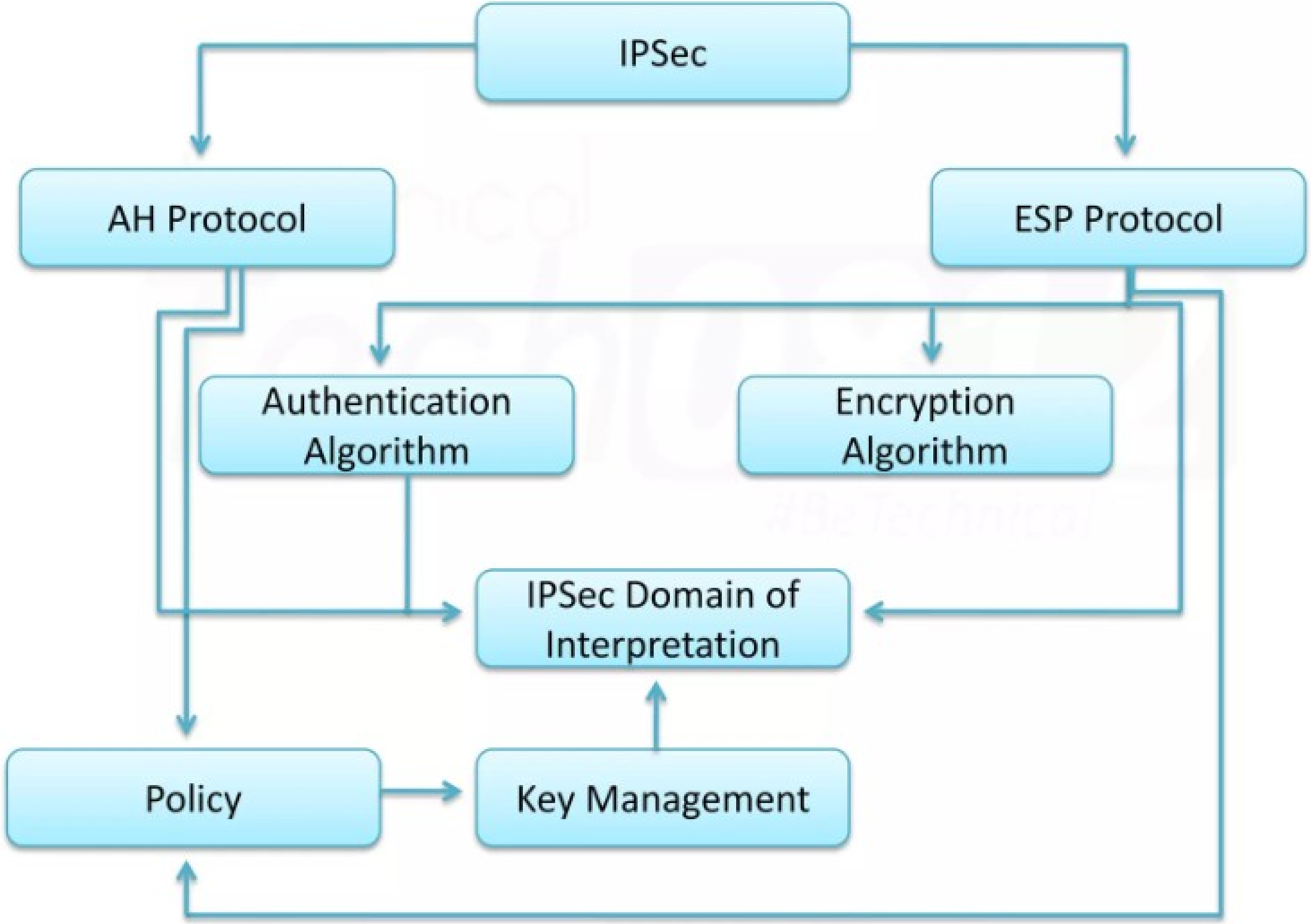

IPSEC (AH and ESP) Modes
Transfer Mode
A
Router 1
Public
Nework
Router 2
B
Tunnel Mode

Uses of IP Security

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide different security options like integrity and authentication without encryption, integrity and authentication with encryption
- To protect network data by setting up circuits using IPsec tunnelling in which all data being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Architecture of IPSec



IPSec (IP Security) architecture

- IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture includes protocols, algorithms, Domain of Interpretation(DOI), and Key Management. All these components are very important in order to provide the three main services:
- Confidentiality
- Authenticity
- Integrity

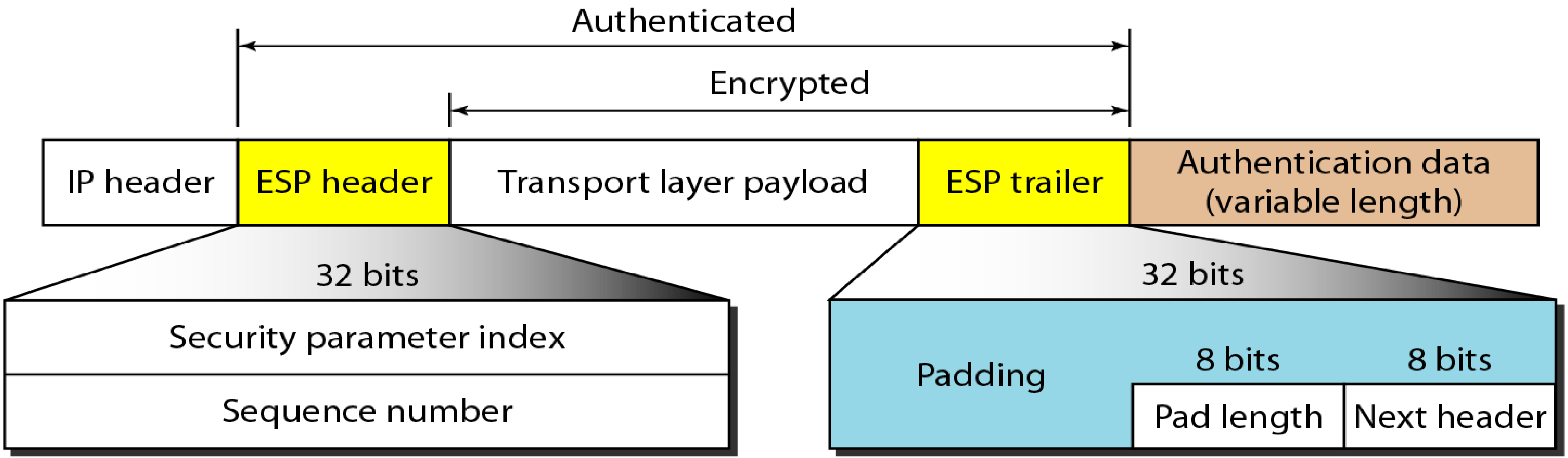
Working on IP Security

- The host checks if the packet should be transmitted using IPsec or not. This packet traffic triggers the security policy for itself. This is done when the system sending the packet applies appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.
- Then IKE Phase 1 starts in which the 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The Main mode provides greater security and the Aggressive mode which enables the host to establish an IPsec circuit more quickly.
- The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.
- Now, the IKE Phase 2 is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agree on secret keying material to be used with those algorithms.
- Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
- When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both hosts.

ESP(Encapsulation Security Payload)

- **ESP Protocol:** ESP(Encapsulation Security Payload) provides a confidentiality service. Encapsulation Security Payload is implemented in either two ways:
- ESP with optional Authentication.
- ESP with Authentication.

Encapsulating Security Payload (ESP) Packet Format



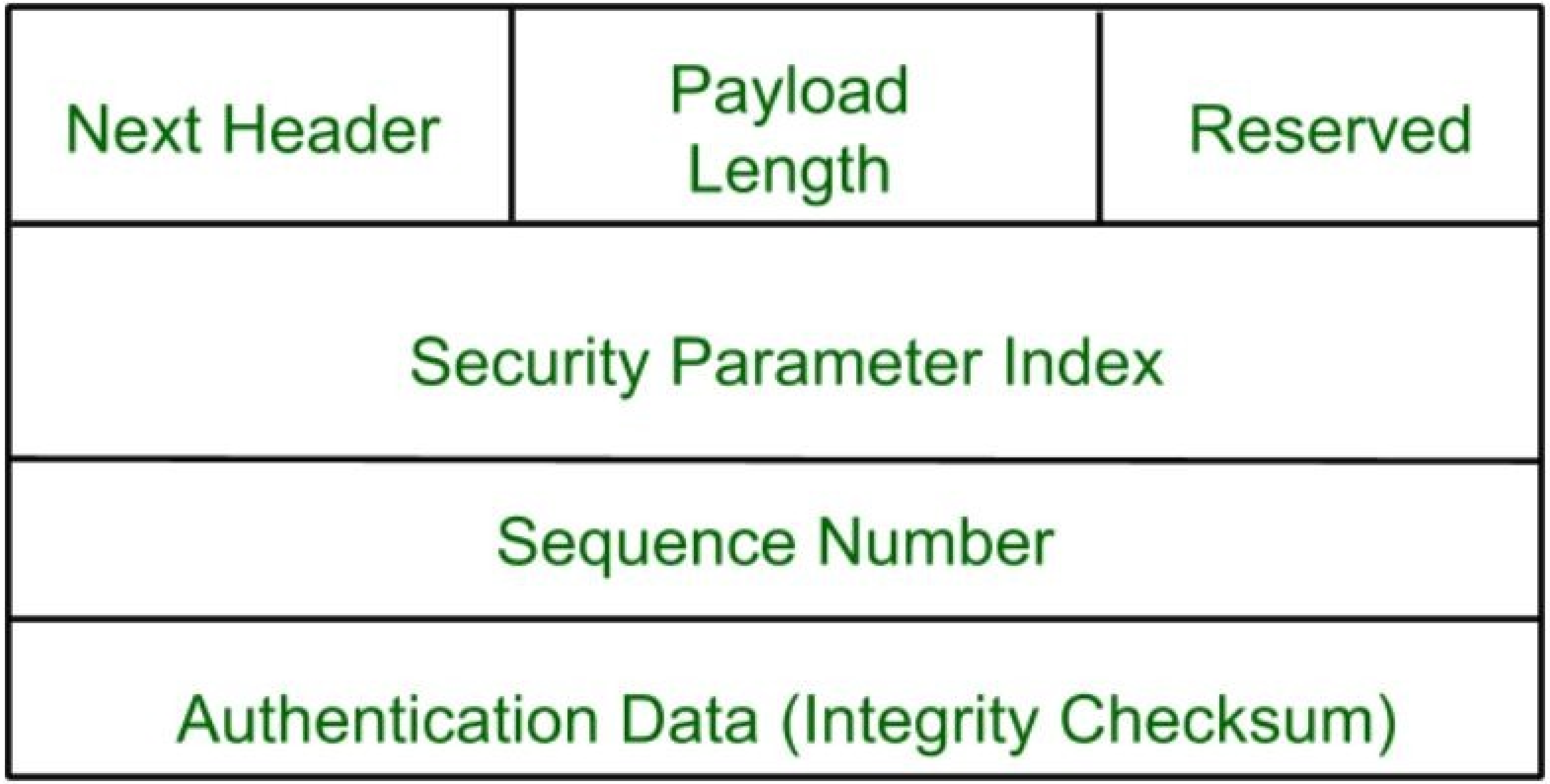
ESP Packet Format Fields

- **Security Parameter Index(SPI):** This parameter is used by the Security Association. It is used to give a unique number to the connection built between the Client and Server.
- **Sequence Number:** Unique Sequence numbers are allotted to every packet so that on the receiver side packets can be arranged properly.
- **Payload Data:** Payload data means the actual data or the actual message. The Payload data is in an encrypted format to achieve confidentiality.
- **Padding:** Extra bits of space are added to the original message to ensure confidentiality. Padding length is the size of the added bits of space in the original message.
- **Next Header:** Next header means the next payload or next actual data.
- **Authentication Data** This field is optional in ESP protocol packet format.

AH (Authentication Header)

- **AH Protocol:** AH (Authentication Header) Protocol provides both Authentication and Integrity services.
- Authentication Header is implemented in one way only:
  - Authentication along with Integrity.

AH Packet Format



Next Header	Payload Length	Reserved
Security Parameter Index		
Sequence Number		
Authentication Data (Integrity Checksum)		

IPSec Authentication Header (AH)

- ***Next header***: the 8-bit next-header field defines the type of payload carried by the IP datagram (such as TCP, UDP, ICMP,..).

- ***Payload length:*** it defines the length of the authentication header

- ***Security Parameter index:*** the 32-bit security parameter index (SPI) is same for all packets sent during a connection called a security association.

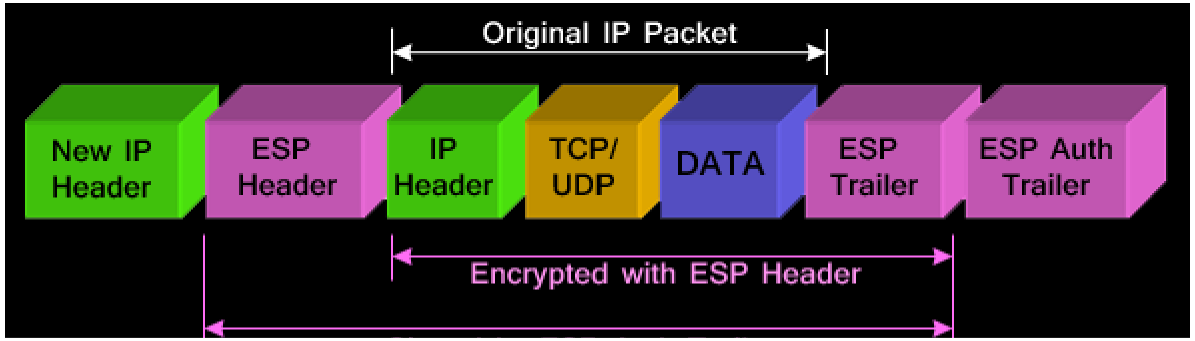
- ***Sequence number:*** the 32-bit sequence number provides ordering information for a sequence of datagram.

- ***Authentication data:*** Authentication data field is the result of applying a hash function to the entire IP datagram except for the field that are changed during transit e.g. time-to-live.

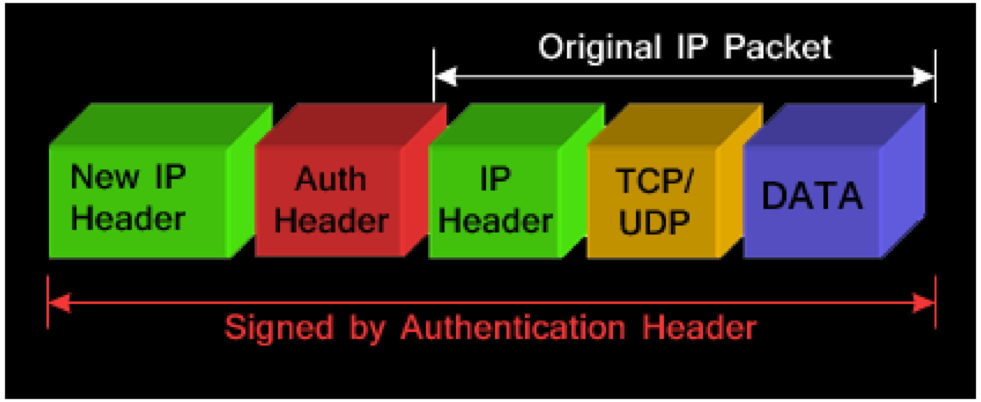
Tunnel mode with ESP or AH

- In tunnel mode, an IPSec header (**AH** or **ESP header**) is inserted between the IP header and the upper layer protocol.
- Between AH and ESP, ESP is most commonly used in IPSec VPN Tunnel configuration.
- ESP is identified in the **New IP header** with an IP **protocol ID** of 50.
- The AH can be applied alone or together with the ESP when IPSec is in tunnel mode.
- AH’s job is to protect the entire packet.
- The AH does not protect all of the fields in the New IP Header
- The AH protects everything that does not change in transit. AH is identified in the New IP header with an IP protocol ID of 51.
- In both ESP and AH cases with IPSec Transport mode, the IP header is exposed.

The packet diagram below illustrates **IPSec Tunnel mode** with **ESP header**:



The packet diagram below illustrates **IPSec Tunnel mode** with **AH header**:



IPSec Modes

1- Transport mode:

- IPSec protects the message passed down to IP from the transport layer. The message is processed by AH and /or ESP and the appropriate headers are added.

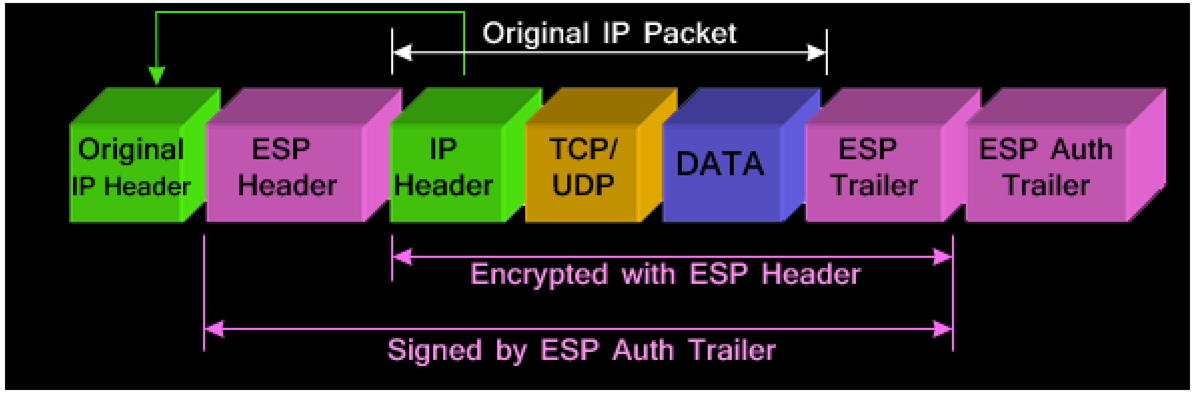
- IPSec in the transport mode does not protect the IP header; it only protects the information coming from the transport layer.

- The transport mode is normally used when we need host-to-host protection of data.

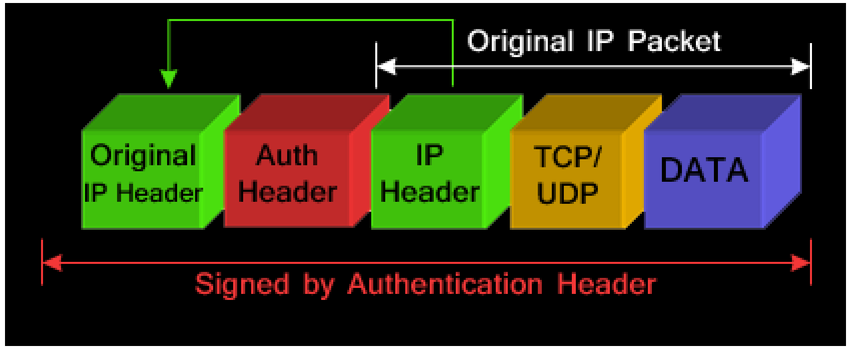
Transport mode with ESP or AH

- IPSec Transport mode is used for end-to-end communications, for example, for communication between a client and a server or between a workstation and a gateway (if the gateway is being treated as a host).
- A good example would be an encrypted Telnet or Remote Desktop session from a workstation to a server.
- Transport mode protects IP Payload through an AH or ESP header.
- The payload is encapsulated by the IPSec headers and trailers.
- The original IP headers remain intact, except that the IP protocol field is changed to ESP (50) or AH (51), and the original protocol value is saved in the IPsec trailer to be restored when the packet is decrypted.
- IPSec transport mode is usually used when another tunnelling protocol is used to first encapsulate the IP data packet and then IPSec is used to protect the tunnel packets.

The packet diagram below illustrates **IPSec Transport mode** with **ESP header**:



The packet diagram below illustrates **IPSec Transport mode** with **AH header**:



IPSec (IP Security) architecture (continued…)

- **Encryption algorithm: The encryption** algorithm is the document that describes various encryption algorithms used for Encapsulation Security Payload.
  - IPSec supports various types of encryptions, including AES, Blowfish, Triple DES, ChaCha, and DES-CBC. IPSec uses asymmetric and symmetric encryption to provide speed and security during data transfer. In asymmetric encryption, the encryption key is made public while the decryption key is kept private.
- **Authentication Algorithm:** The authentication Algorithm contains the set of documents that describe the authentication algorithm used for AH and for the authentication option of ESP.

  Authentication algorithms
  - RSA
  - ECDSA (RFC 4754)
  - PSK (RFC 6617)
  - EdDSA (RFC 8420)
- **DOI (Domain of Interpretation):** DOI is the identifier that supports both AH and ESP protocols. It contains values needed for documentation related to each other.
- **Key Management:** Key Management contains the document that describes how the keys are exchanged between sender and receiver.

Advantages of IPSec

- **Strong security:** IPSec provides strong cryptographic security services that help protect sensitive data and ensure network privacy and integrity.
- **Wide compatibility:** IPSec is an open standard protocol that is widely supported by vendors and can be used in heterogeneous environments.
- **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
- **Scalability:** IPSec can be used to secure large-scale networks and can be scaled up or down as needed.
- **Improved network performance:** IPSec can help improve network performance by reducing network congestion and improving network efficiency.

Disadvantages of IPSec

- **Configuration Complexity:** IPSec can be complex to configure and requires specialized knowledge and skills.
- **Compatibility Issues:** IPSec can have compatibility issues with some network devices and applications, which can lead to interoperability problems.
- **Performance Impact:** IPSec can impact network performance due to the overhead of encryption and decryption of IP packets.
- **Key Management:** IPSec requires effective key management to ensure the security of the cryptographic keys used for encryption and authentication.
- **Limited Protection:** IPSec only protects IP traffic, and other protocols such as ICMP, DNS, and routing protocols may still be vulnerable to attacks.