**What is Encapsulating Security Payload ?**

* Cyber Security is the branch of computer technology that deals with the security of the virtual cloud and internet.
* Any information that is stored or transmitted through the cloud needs to be secure and safe.
* Cyber Networking plays a very important role in maintaining that the connection established is secured and content goes through a safe channel for transmission.

**The structure of ESP, and its importance in security:**

* IPSec uses security algorithms like SHA and MD5 to protect data.
* Each packet is uniquely identified and authenticated to ensure it’s secure.
* The Encapsulating Security Payload (ESP) protocol is a key part of IPSec.
* ESP ensures Confidentiality (data is hidden), Integrity (data isn’t changed), and Availability (data is accessible to the right user).
* Only verified users can encrypt and decrypt the data, ensuring it stays safe from hackers or unauthorized access.

**Working of ESP:**

1. **Protocol Support:** ESP works with both **IPv4** and **IPv6** network protocols.
2. **Encryption Role:** It encrypts data and adds a security layer within the **IP header**, protecting the transmitted information.
3. **Position in the Network Stack:** ESP is placed **between the IP protocol** and higher-level protocols like **UDP, TCP, or ICMP**, ensuring that the data payload is secure before it reaches its final destination.

**Modes in ESP (Encapsulating Security Payload):**

1. **Tunnel Mode:**

Commonly used between network gateways (e.g., router-to-router).

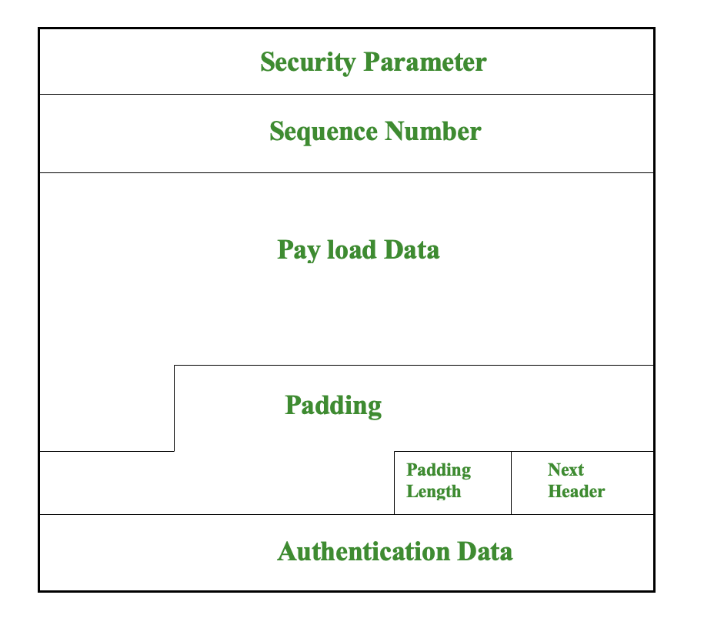
A new IP header is created and added outside the original packet, followed by ESP.

1. **Transport Mode:**

Typically used for end-to-end communication (e.g., between two devices).

Only the payload (data) is encrypted and authenticated, while the IP header remains unprotected.

**Components of ESP:**



1. **Security Parameter Index(SPI):** It is used to give a unique number to the connection built between the Client and Server.
2. **Sequence Number:** Unique Sequence numbers are allotted to every packet so that on the receiver side packets can be arranged properly.
3. **Payload Data:** Payload data means the actual data or the actual message. The Payload data is in an encrypted format to achieve confidentiality.
4. **Padding:** Extra bits of space are added to the original message in order to ensure confidentiality. Padding length is the size of the added bits of space in the original message.
5. **Pad Length:** Indicates the **number of padding bytes** added before the payload.
6. **Next Header:** Next header means the next payload or next actual data.
7. **Authentication Data :** An **optional field** ensuring **data integrity**, used when Security Association (SA) is active.

**Advantages:**

1. Encrypting data to provide security
2. Maintaining a secure gateway for data/ message transmission
3. Properly authenticating the origin of data
4. Providing needed data integrity
5. Maintaining data confidentiality