Internet Protocol Security

Tasnimul Hasnat
19004113

What is IP Security ?

IP Security (IPSec) is a collection of protocols designed by the **Internet Engineering Task Force (IETF)** to provide security for a packet at the network level.

Overview

- Security solution in the **network layer** instead of **transport layer (TLS)** or **Application layer (SSH)**.
- Provides security for node to node communication protocols e.g. **routing protocols**.
- Current version defined in **RFC 4301 (2005)**.
- Widely used in **Virtual Private Networks (VPN)**.
- Provides authentication and integrity for **packet sources**.
- Authentication and confidentiality(**encapsulation**) can be used separately or together.
- Prevents
  - IP Spoofing
  - Eavesdropping
  - Denial of service

Overview

Security Architecture

Transport Mode
Tunnel Mode

Data Encapsulation

AH
ESP

Security Association

SAD
SPD

Authenticated Keyring

IKE

Security Architecture

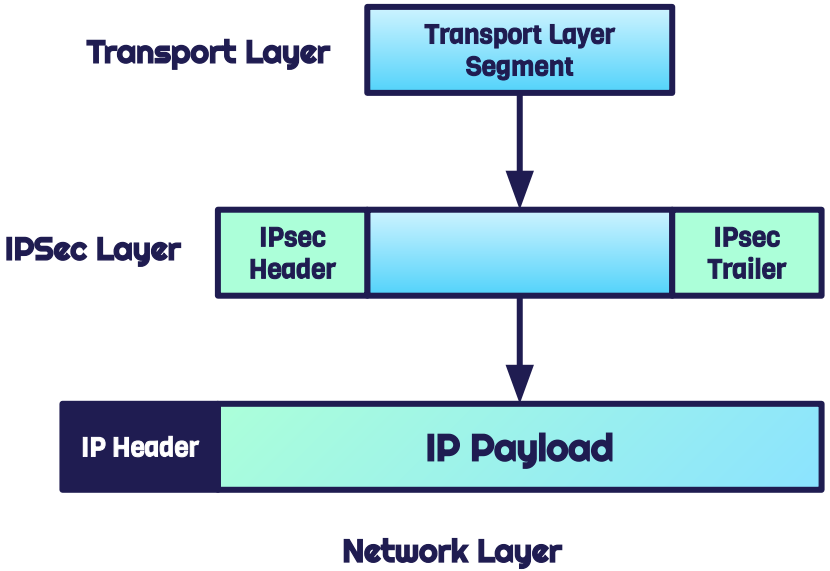
IPSec operates in one of **two** different modes.

Transport Mode
Host to Host

Tunnel Mode
Gateway to Gateway

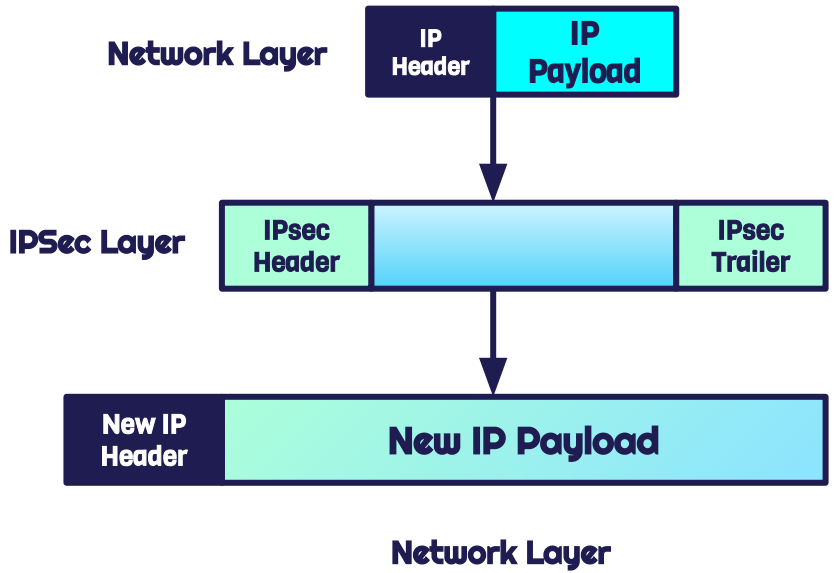
Transport Mode

- End to end protection of data.
- Protects what comes from upper transport layer i.e. IP packet only.
- Does not protect IP header.

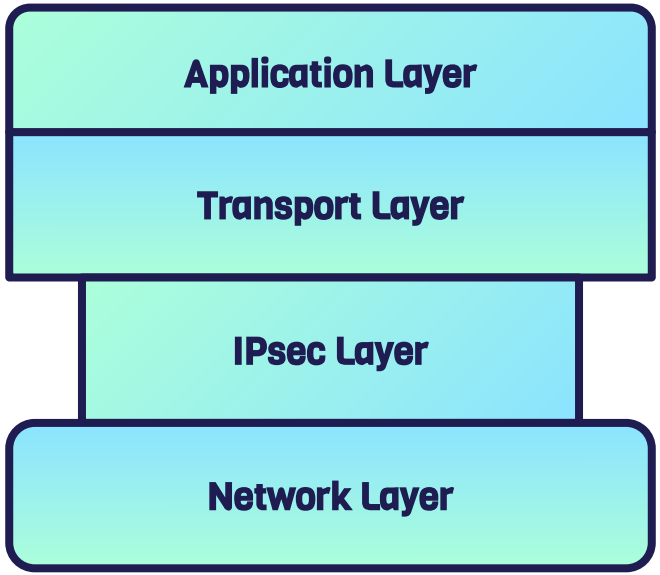


Tunnel Mode

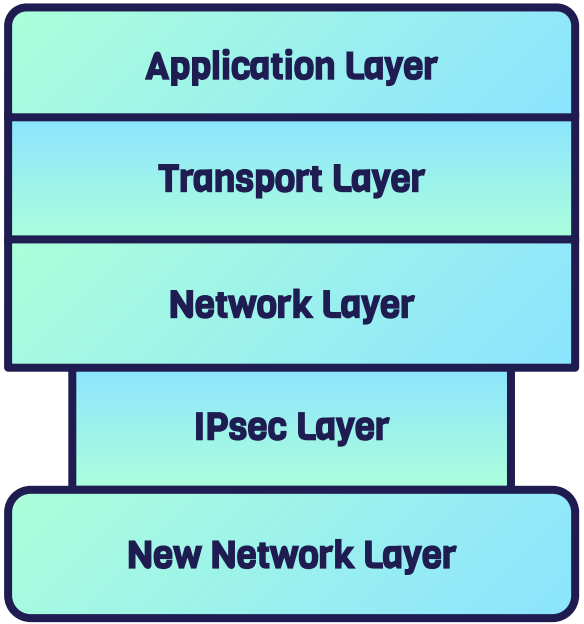
- Router to router, router to host or vice-versa protection of data.
- Protects entire IP packet also with the IP header.
- Adds a new IP header with different information from the previous one.



Comparison



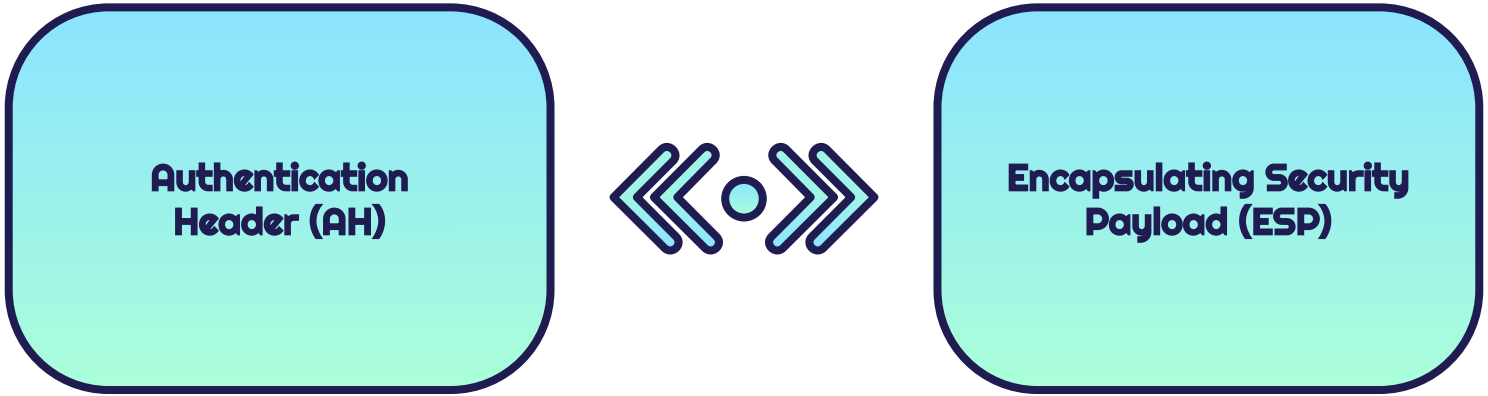
Transport Mode



Tunnel Mode

Data Encapsulation

IPSec defines two protocols to provide authentication and/or encryption.



danke