Hello Everyone! In this video, you will learn about IP Security protocol. It is called IPSec in Short.

In today's cyber world, where cyber-attacks are increasing day by day and attackers are becoming more powerful, it is not enough to provide security on application layer only. Therefore, it becomes necessary to provide security at various layers. IP Sec is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level.
IPSec helps create authenticated and confidential packets for the IP layer.

IPSec may operate in two different modes, Tunnel mode and Transport mode. IPSec Transport mode is used for securing the payload of IP packets that is the data coming from transport layer, while in tunnel mode IPSec protects the complete IP packet including header.

IPSec Is the collection of two security protocols.
Authentication Header Protocol and Encapsulated Security Protocol for providing a different set of security features to the applications.

The Authentication Header (AH) protocol provides data integrity and authentication. it does not provide encryption. Therefore, it does not provide data confidentiality. AH was designed to be inserted into an IP packet to add authentication data and protect the contents

from modification. This protocol is now obsolete and supported by only legacy applications.

Encapsulating Security Payload (ESP) provides data integrity, encryption and authentication. This protocol has now replaced the AH protocol for all new implementations., as it provides integrity, authentication and confidentiality features alone.

Here is the difference between the AH and ESP protocols., AH provides Access Control, Message authentication, entity authentication and protection from replay attacks, while ESP provides confidentiality in addition to all the protections provided by AH.

Thank You