

The NPTEL logo is a circular emblem. It features a stylized flower or star shape in the center, composed of several overlapping loops in shades of pink and orange. This central motif is surrounded by a circular border made of small, rectangular segments in alternating orange and pink colors, creating a ring-like effect.

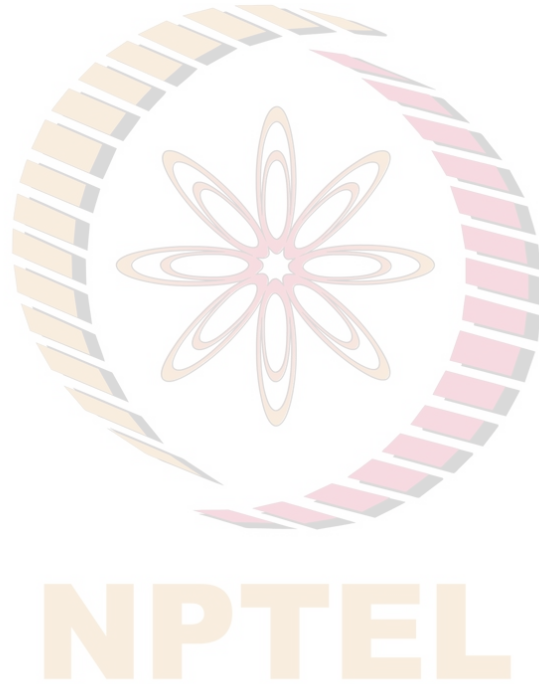
IP Security

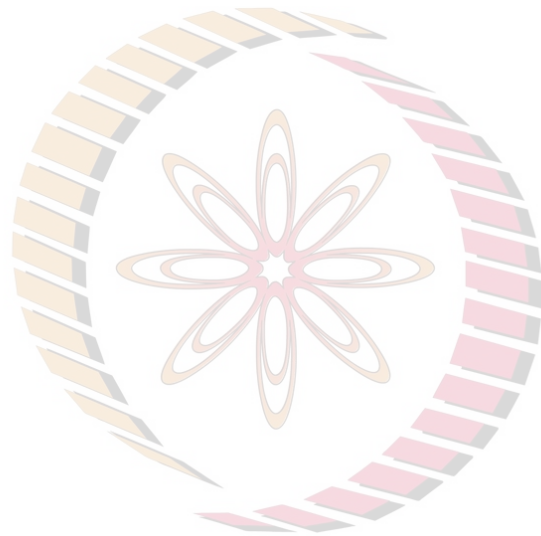
Dr. Neminath Hubballi

NPTEL

Overview

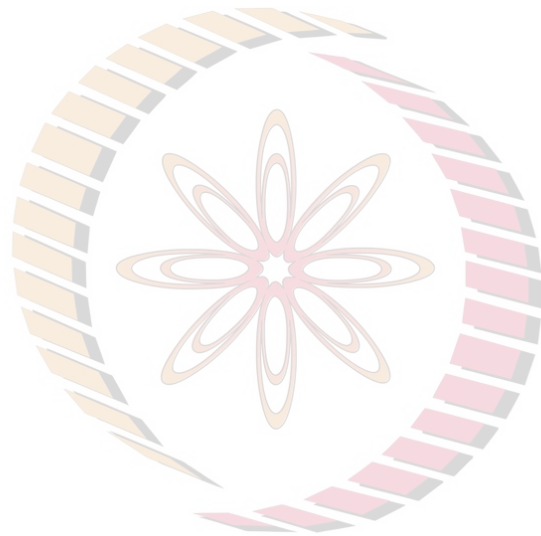
- ☐ Background
- ☐ IPSec features
- ☐ Deployment scenarios
- ☐ Components
- ☐ Methods
- ☐ Security Association





NPTEL

Indian Institute of Technology Indore



NPTEL

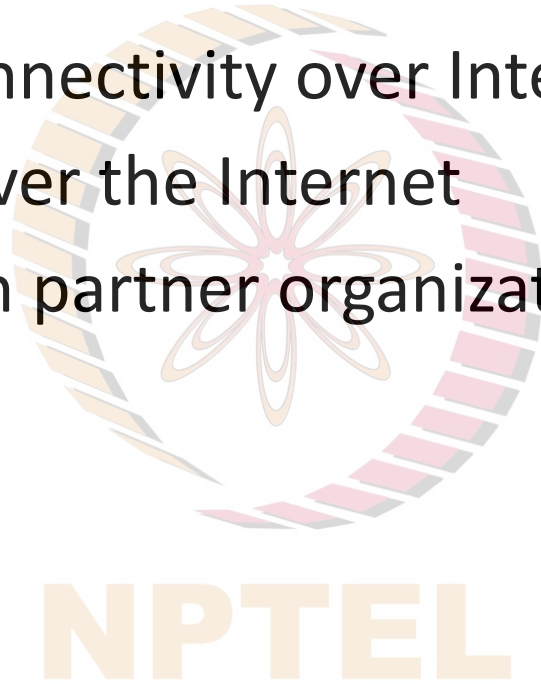
Indian Institute of Technology Indore

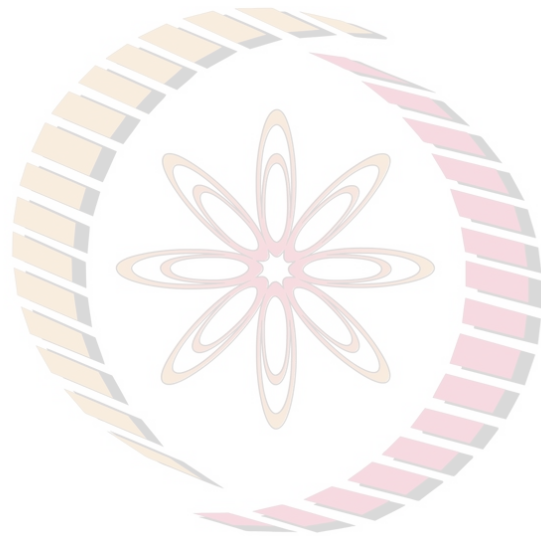
IPSec Features

- ☐ Encrypt and authenticate network traffic at the IP layer
 - ☐ Several networked applications can be secured
- ☐ Data origin authentication: Each IP datagram was originated by the claimed sender.
- ☐ Data integrity: IP datagram was not modified in transit
- ☐ Data confidentiality: Conceals the content of a message, typically by using encryption.
- ☐ Replay protection: Capture and retransmit is not allowed
- ☐ Automated management of cryptographic keys and security associations: Ensures that your VPN policy can be used throughout the extended network with little or no manual configuration.

Use cases

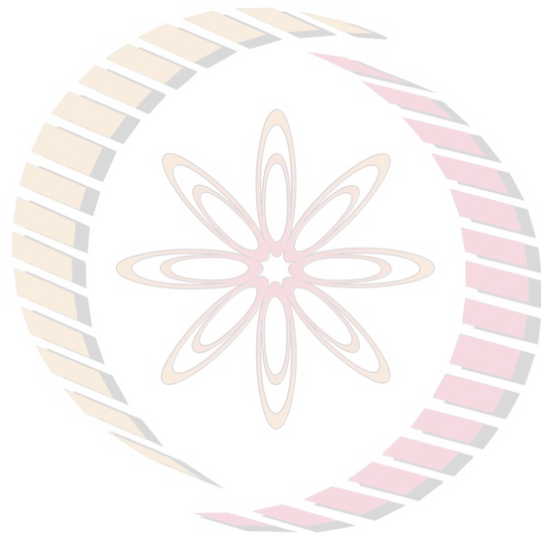
- ☐ Secure branch office connectivity over Internet
- ☐ Secure remote access over the Internet
- ☐ Secure connections with partner organizations





NPTEL

Indian Institute of Technology Indore

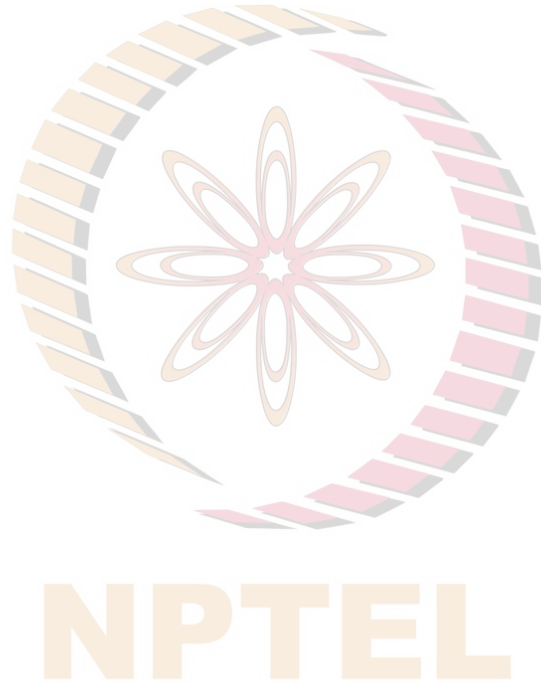


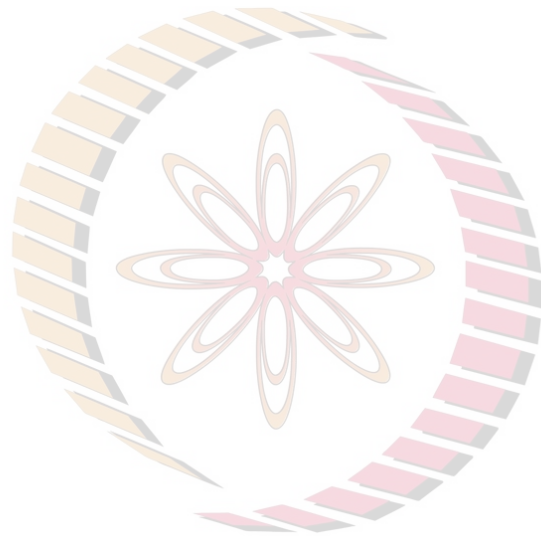
NPTEL

Indian Institute of Technology Indore

Where to Implement IPSec Methods ?

- ☐ End host or
- ☐ Middlebox





NPTEL

Indian Institute of Technology Indore

IPSec -Two Methods

- ❑ Authentication Header (AH): Provides authentication through an extended/extra header.
 - ❑ Deprecated as ESP provides both confidentiality and authentication
- ❑ Encapsulating Security Payload(ESP): Provides confidentiality and confidentiality along with authentication.

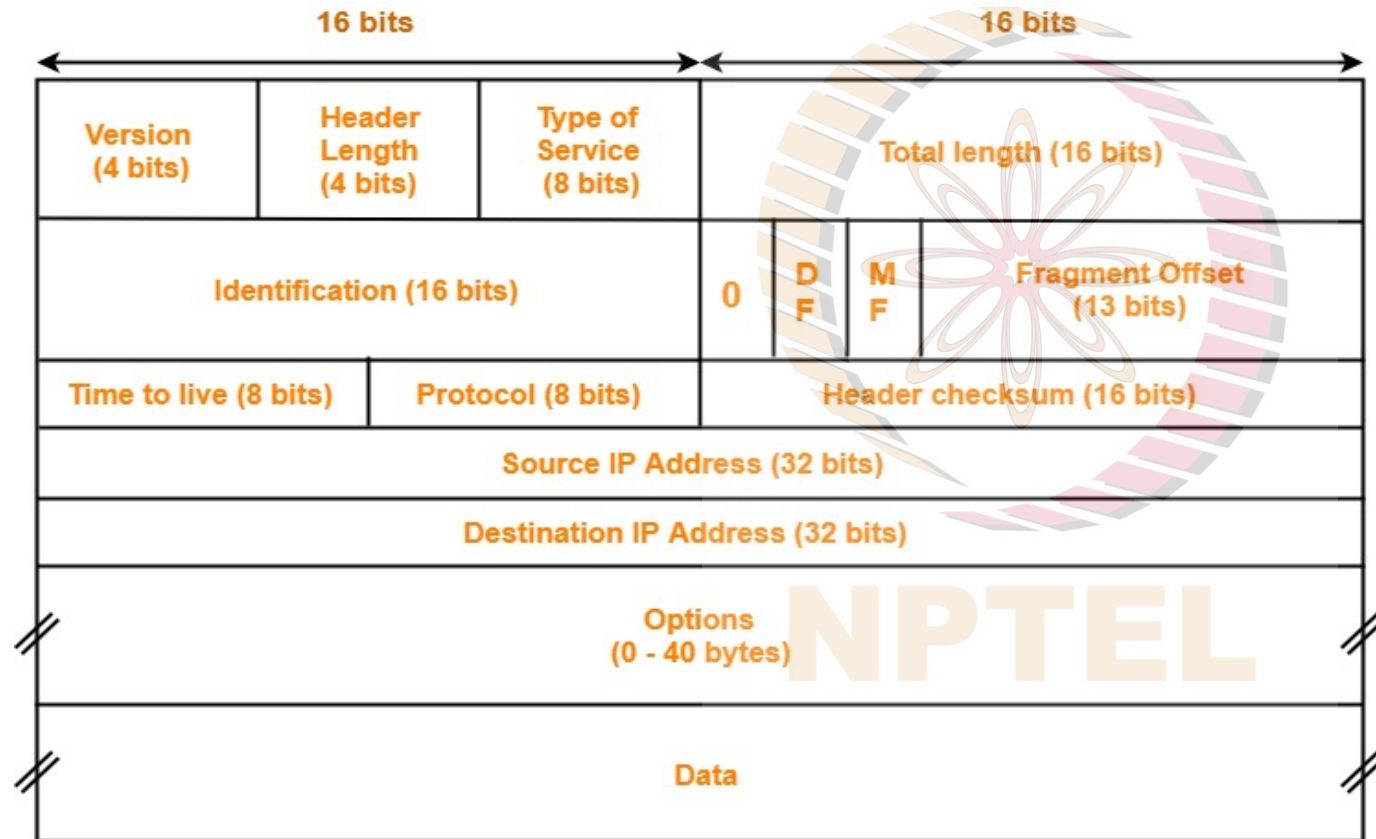
NPTEL

IPSec Modes

- ❑ Transport Mode: Secure the data given by a protocol above IP
 - ❑ IPSec header is inserted into the original IP header
- ❑ Tunnel Mode: Original IP packet is encrypted and sent
 - ❑ A new IP header is inserted at the beginning

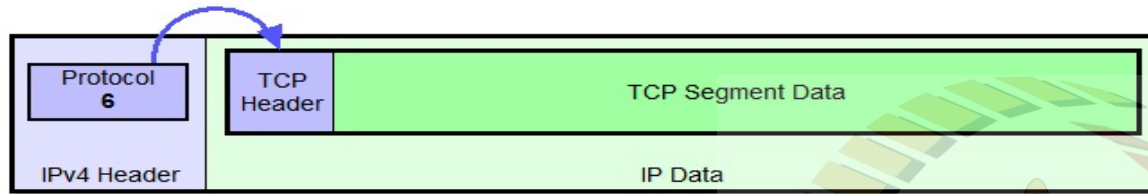
NPTEL

IPv4 Header Format



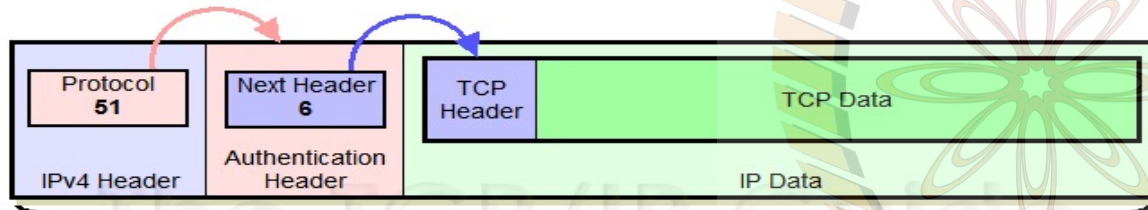
IPv4 Header

Authentication Header and IPv4



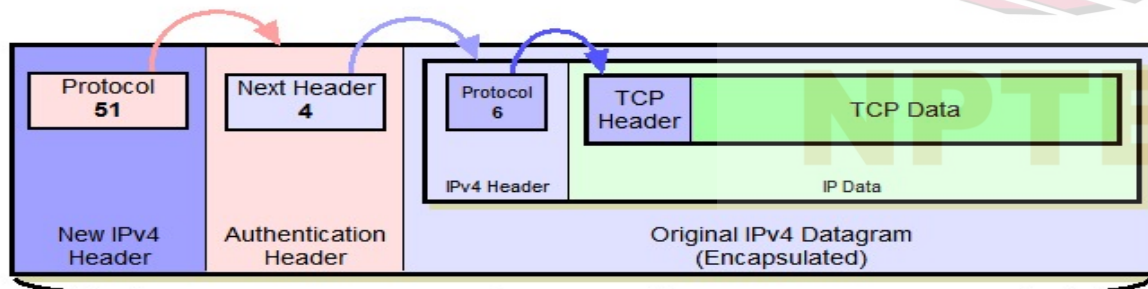
Original IPv4 Datagram Format

Courtesy: tcpguide.com



Authenticated Fields

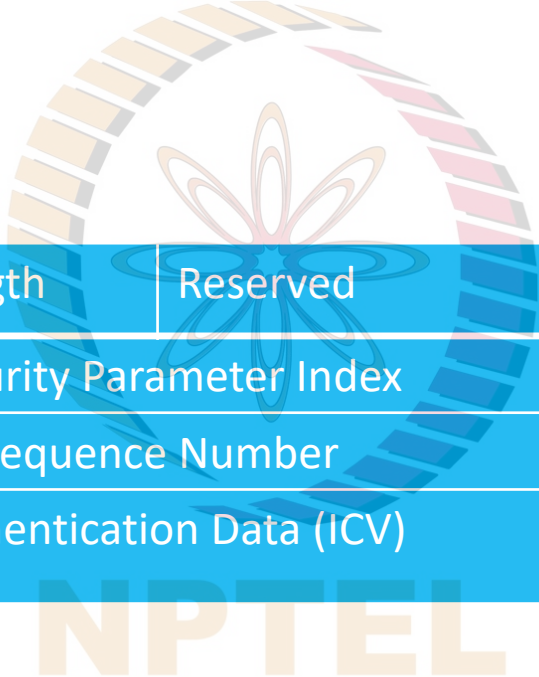
IPv4 AH Datagram Format - IPsec Transport Mode



Authenticated Fields

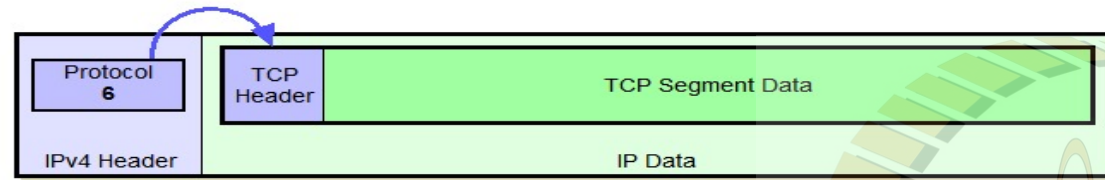
IPv4 AH Datagram Format - IPsec Tunnel Mode

Authentication Header Format



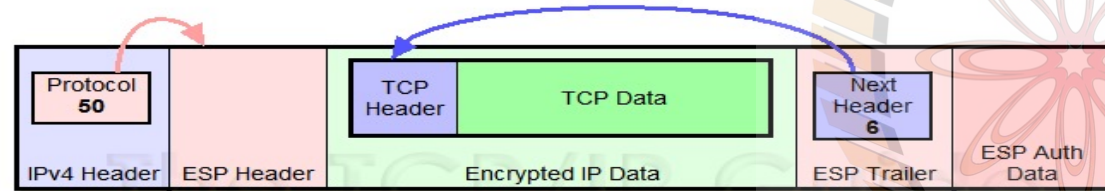
Next Header	Payload Length	Reserved
Security Parameter Index		
Sequence Number		
Authentication Data (ICV)		

Encapsulating Security Payload

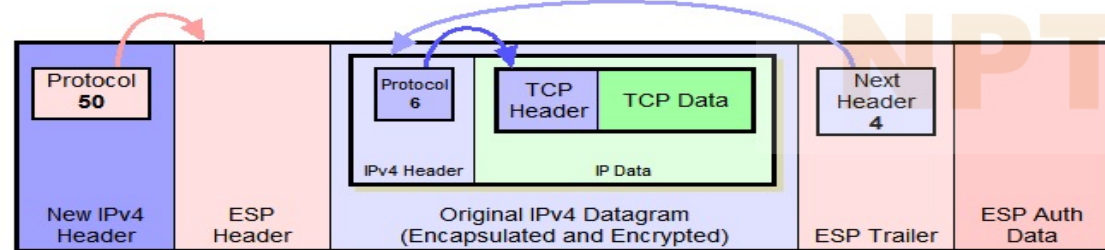


Original IPv4 Datagram Format

Courtesy: tcpguide.com

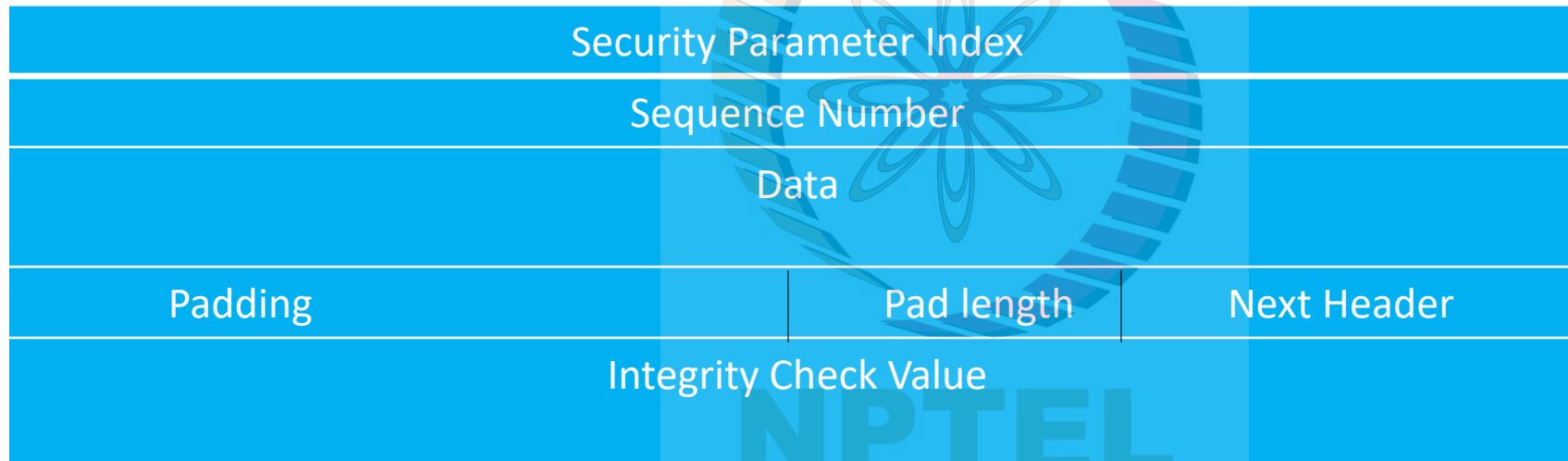


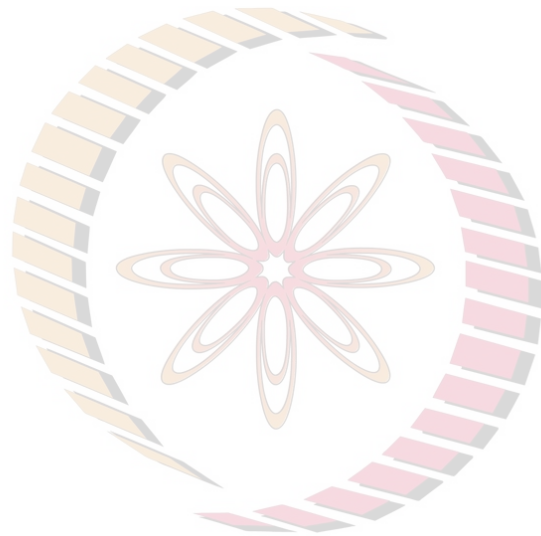
IPv4 ESP Datagram Format - IPsec Transport Mode



IPv4 ESP Datagram Format - IPsec Tunnel Mode

Encapsulating Security Payload





NPTEL

Indian Institute of Technology Indore

IPSec Components

- ☐ Encryptions and Hashing Algorithms

 - ☐ DES, AES

 - ☐ MD5, SHA-1

- ☐ Security Associations

- ☐ Key Exchange Methods



IP Security Policy

☐ Security Association Database (SAD)

☐ A security association is uniquely identified by

- ☐ Security Parameter Index (SPI)- a bit string added to IP packet
- ☐ Destination IP Address
- ☐ Security Protocol Identified – AH or ESP

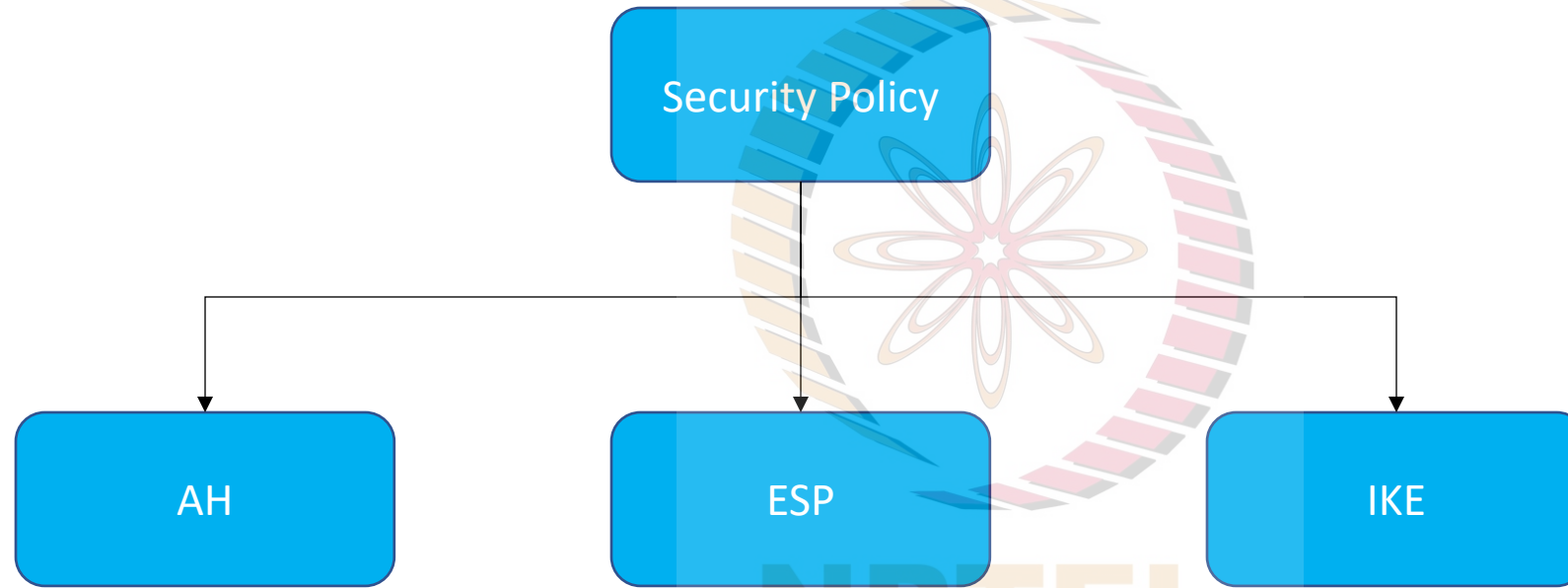
☐ Security Association is One-Way connections

☐ Security Policy Database (SPD)- Determines a SA for a subset of IP traffic

- ☐ Remote IP address
- ☐ Local IP address
- ☐ Higher layer protocol
- ☐ Name
- ☐ Port numbers

NPTTEL

IPSec Architecture



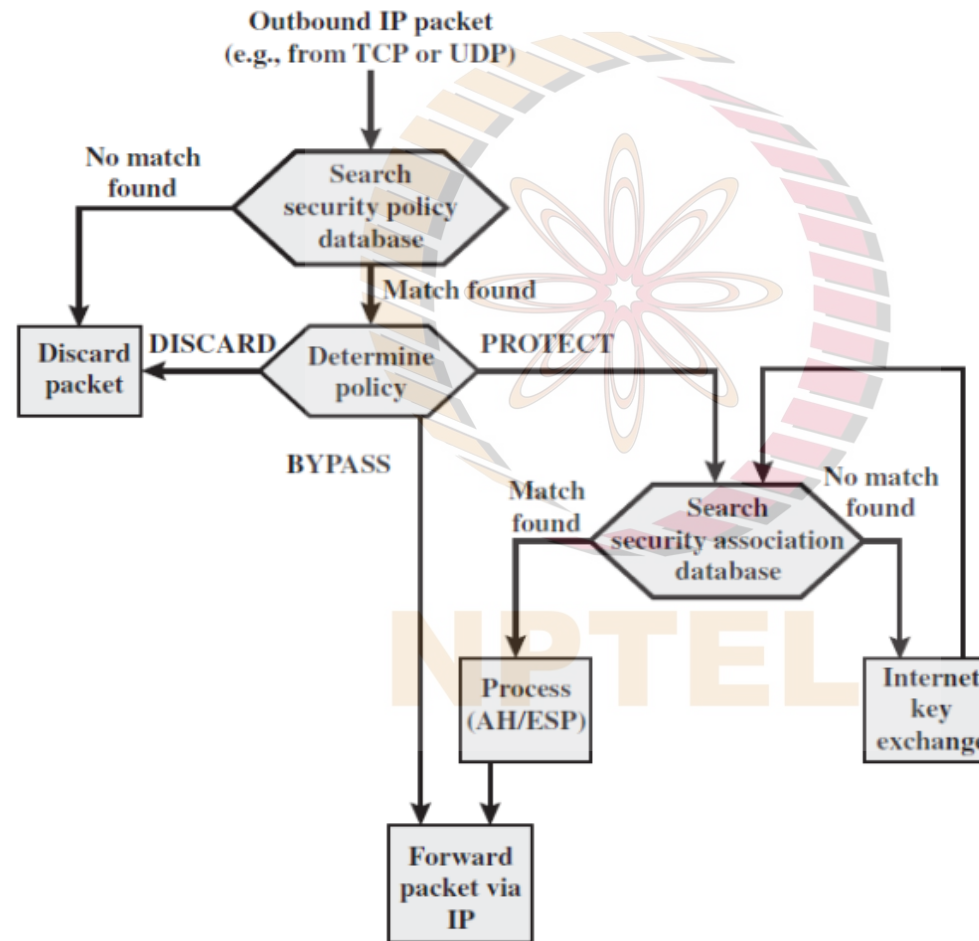
Establishing a Security Association

- ☐ Manually
 - ☐ On each node configuration
 - ☐ Who are the participants of communication
 - ☐ Mode of IPSec
 - ☐ Key to be used
- ☐ Internet Key Exchange (IKE)
 - ☐ Automatic configuration

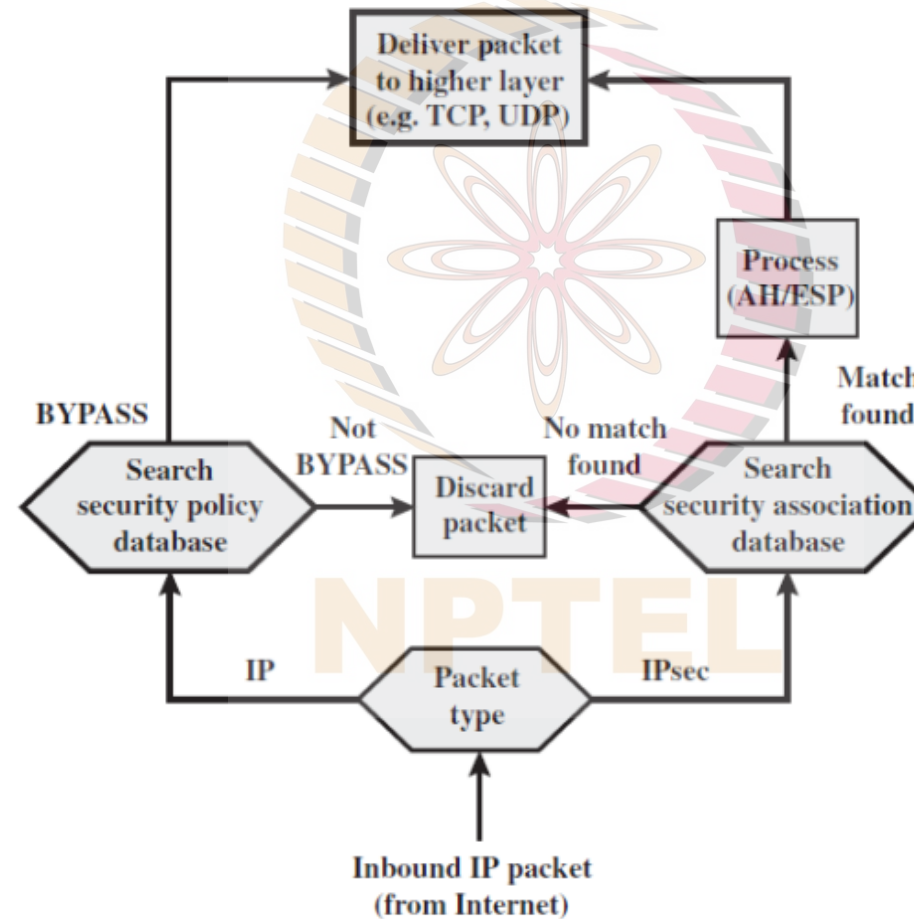


IP Packet Processing: Outbound

Courtesy: Network Security Essentials
By William Stallings



IP Packet Processing: Inbound



Courtesy: Network Security Essentials
By William Stallings