

Protocol Basics

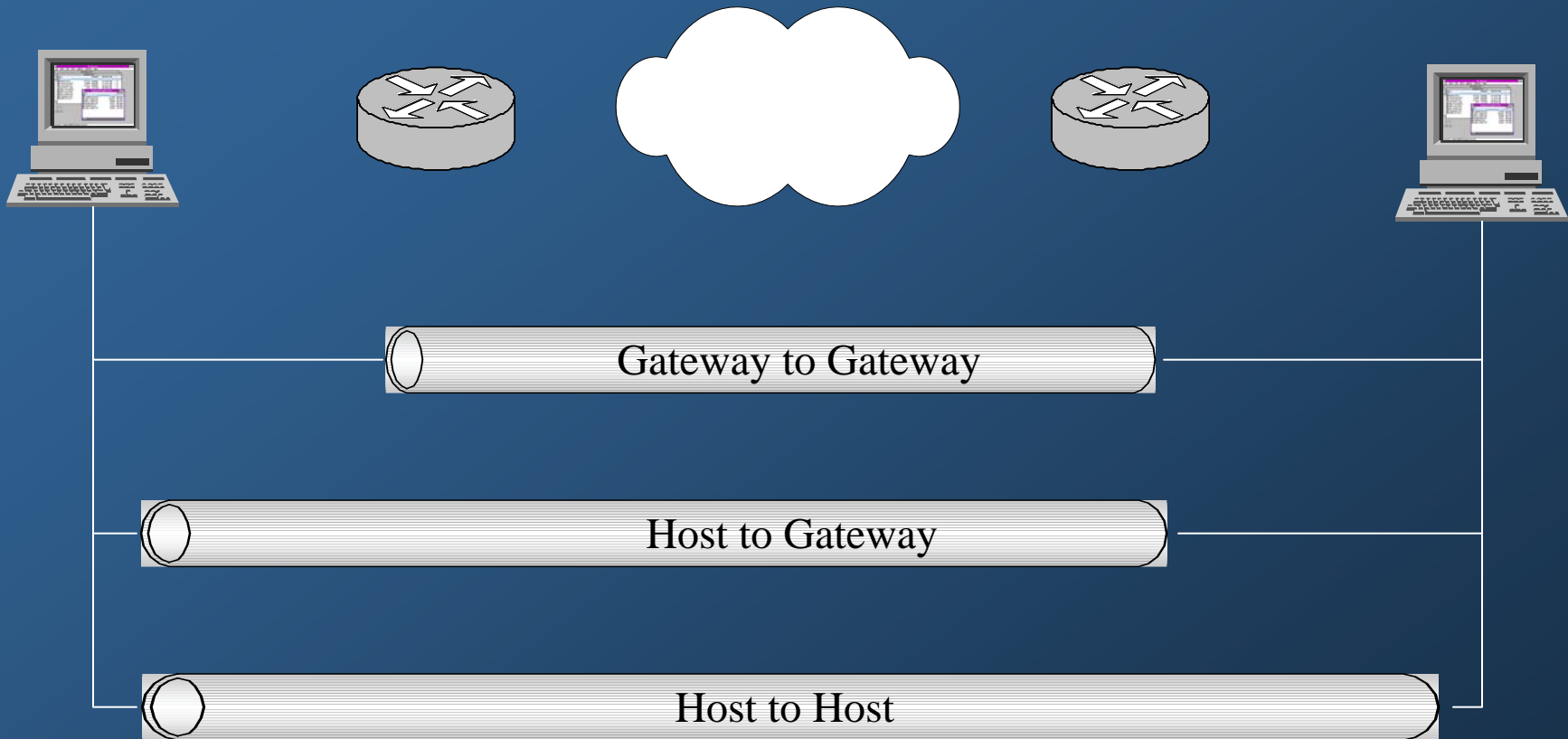
IPSec

- Provides two modes of protection
 - Tunnel Mode
 - Transport Mode
- Authentication and Integrity
- Confidentiality
- Replay Protection

Tunnel Mode

- Encapsulates the entire IP packet within IPSec protection
- Tunnels can be created between several different node types
 - Gateway to gateway
 - Host to gateway
 - Host to host

Three Types of Tunnels



Transport Mode

- Encapsulates only the transport layer information within IPSec protection
- Can only be created between host nodes

Authentication and Integrity

- Verification of the origin of data
- Assurance that data sent is the data received
- Assurance that the network headers have not changed since the data was sent

Confidentiality

- Encrypts data to protect against eavesdropping
- Can hide data source when encryption is used over a tunnel

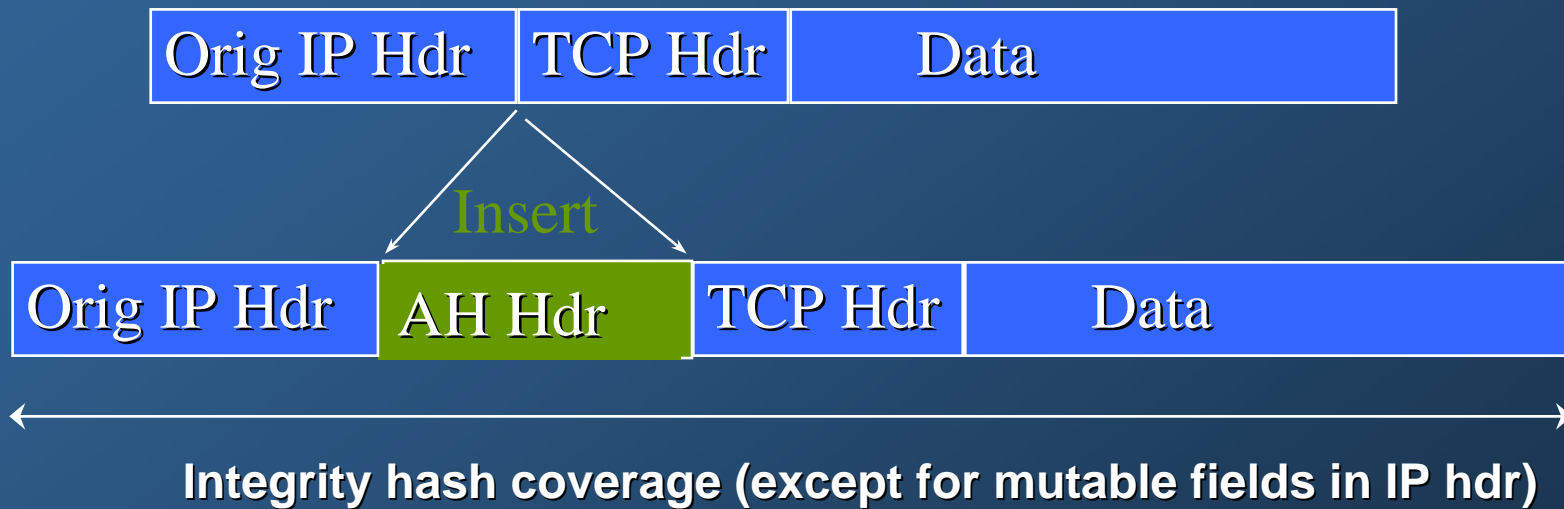
Replay Prevention

- Causes retransmitted packets to be dropped.

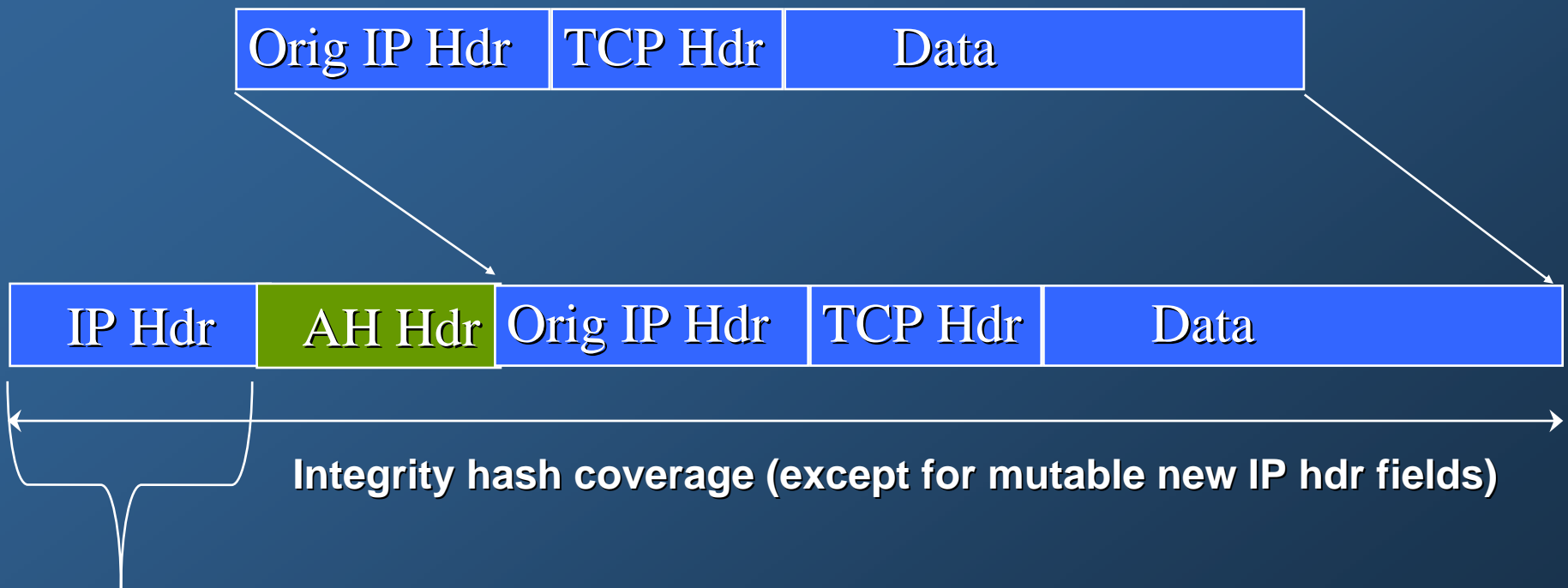
IPSec Protection Protocols

- Authentication Header
 - Authenticates payload data
 - Authenticates network header
 - Gives anti-replay protection
- Encapsulated Security Payload
 - Encrypts payload data
 - Authenticates payload data
 - Gives anti-replay protection

IPSec AH in Transport Mode

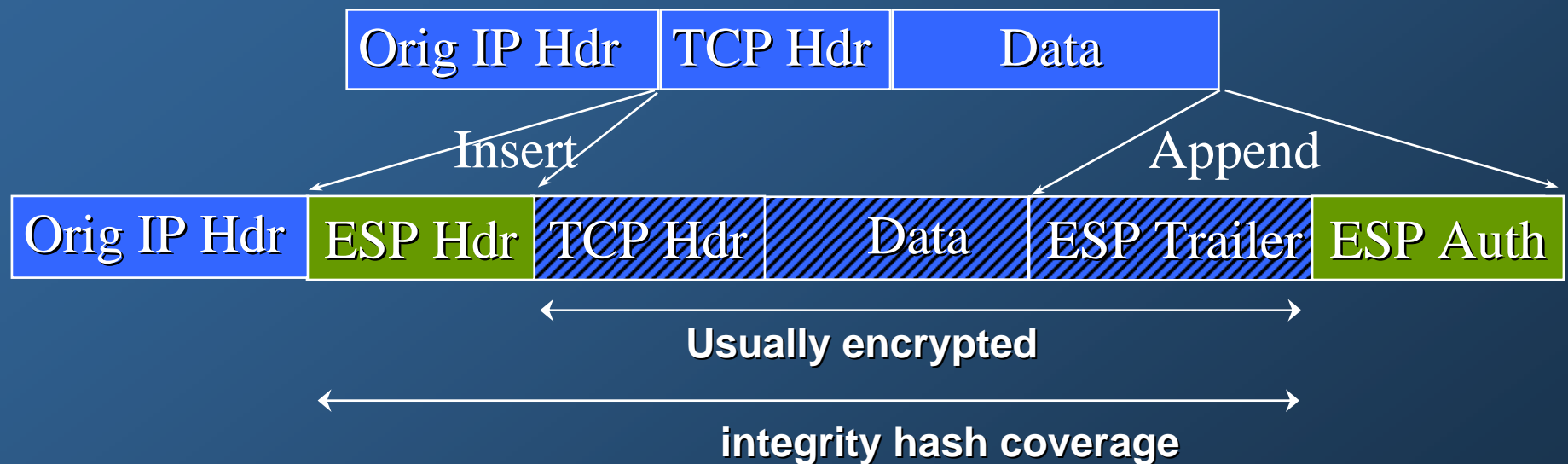


IPSec AH in Tunnel Mode

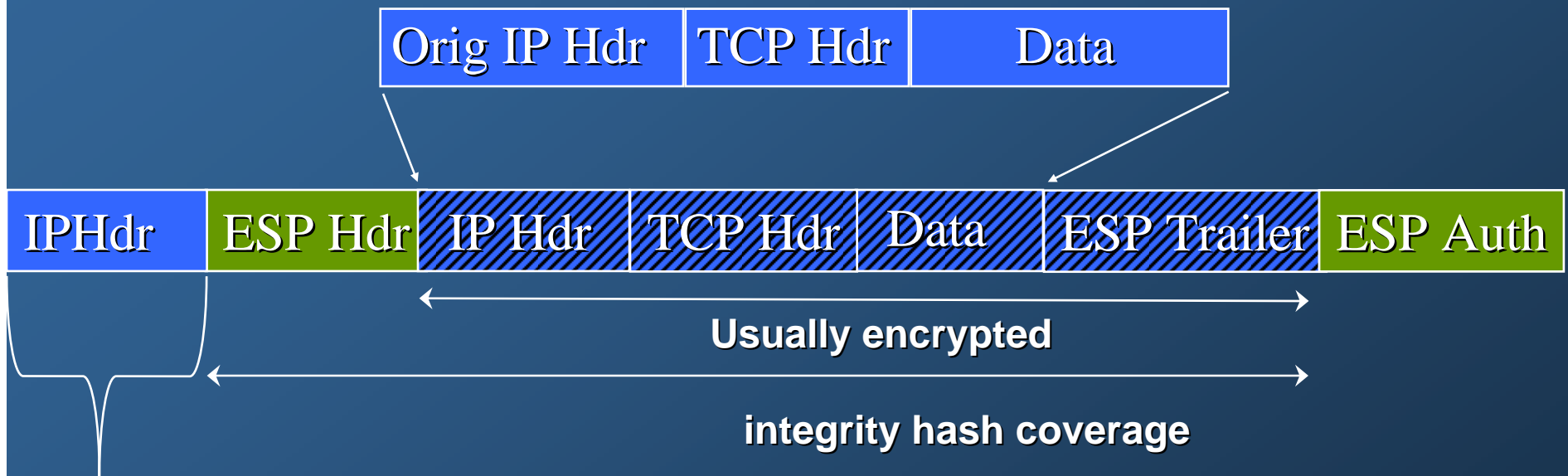


New IP header with source & destination IP address

IPSec ESP in Transport Mode



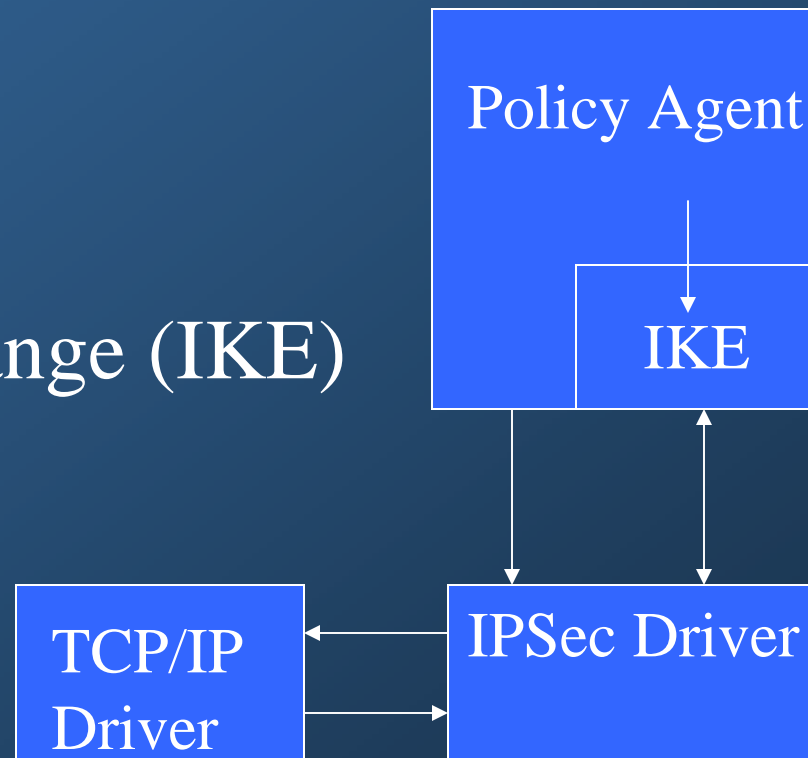
IPSec ESP Tunnel Mode



New IP header with source & destination IP address

IPSec Basic Architecture

- IPSec Driver
- Policy Agent
- Internet Key Exchange (IKE)



IPSec Driver

- Monitors and Secures IP traffic
 - Encryption and Authentication of outbound packets
 - Decryption and Authentication of inbound packets
 - Prompts IKE to negotiate secure channels as needed
- Maintains secure channel state information

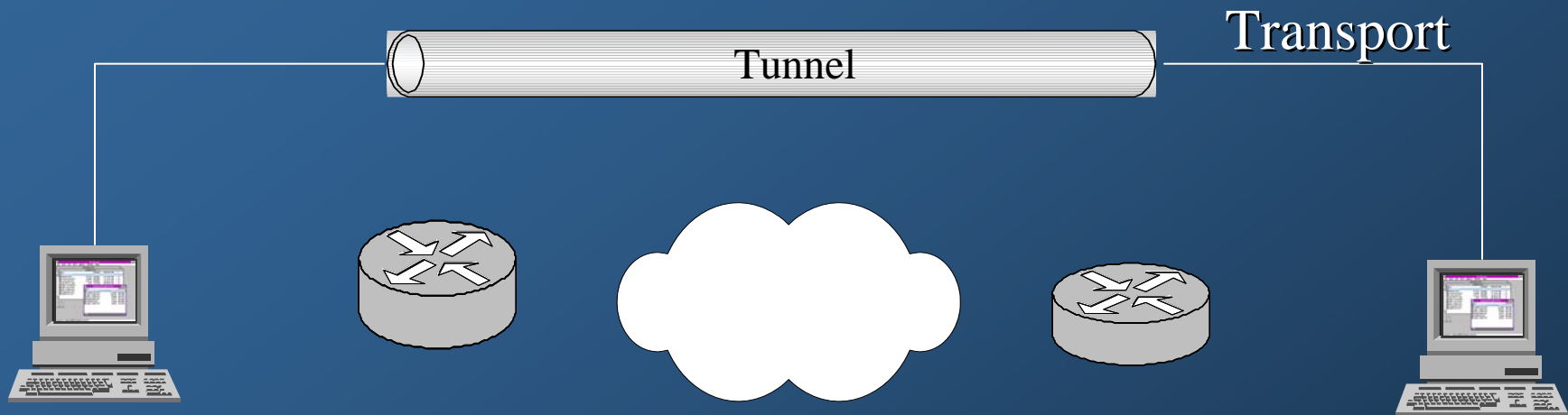
Policy Agent

- Maintains IPSec policy and state information
- Distributes filter rule sets to the IPSec Driver
- Distributes authentication and security settings to IKE

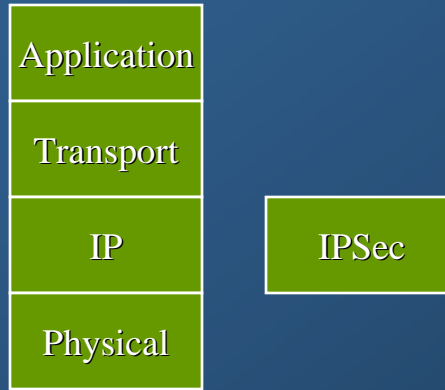
IKE

- Negotiates secure channels based on settings received from the Policy Agent
- Distributes secure channel information to the IPSec driver

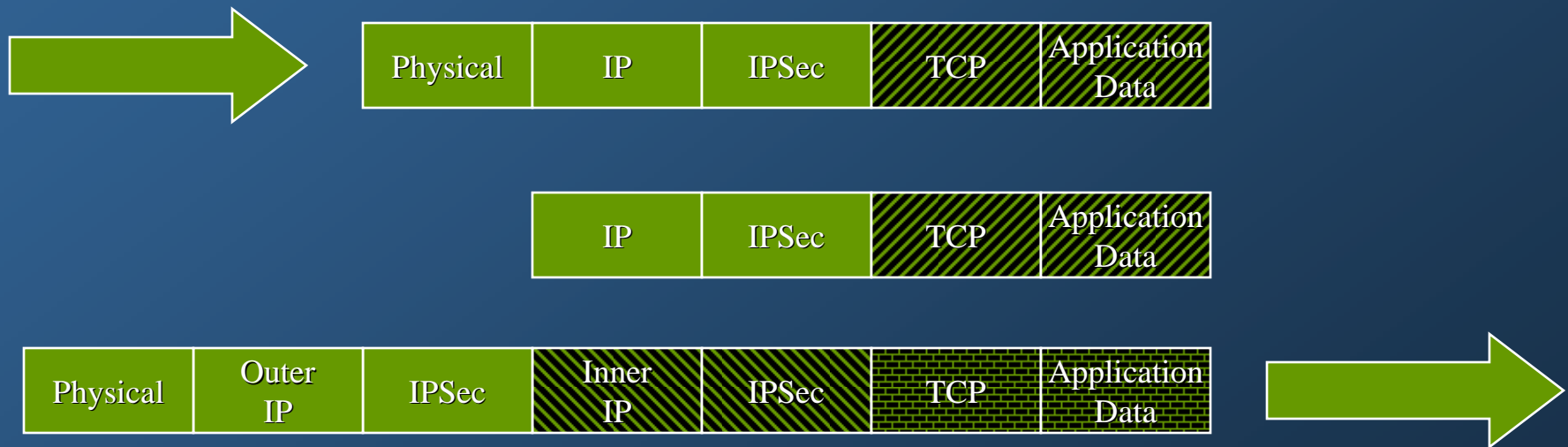
How It All Fits Together



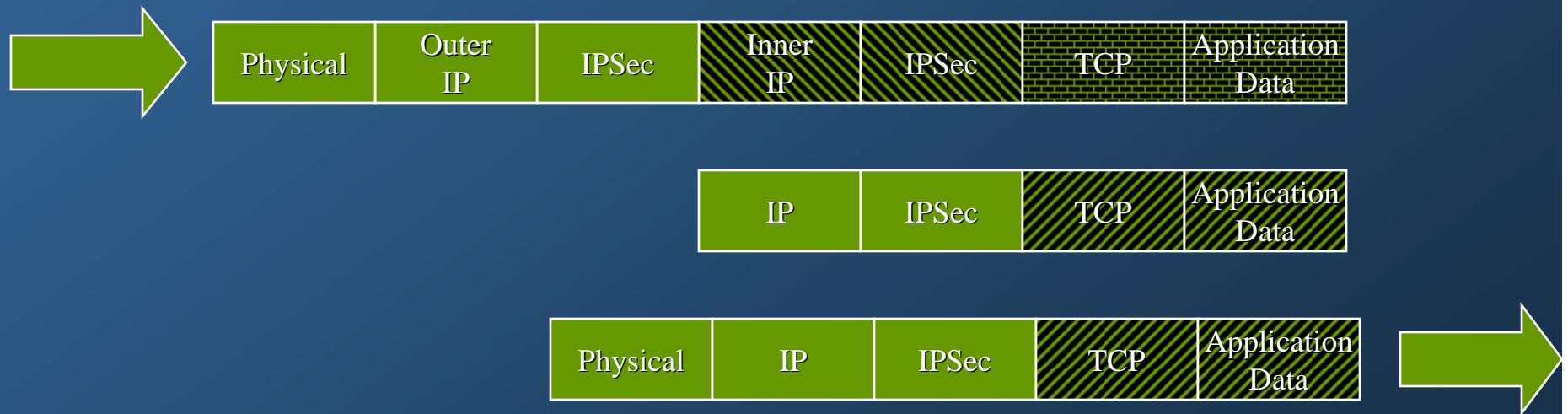
Sending in Transport Mode



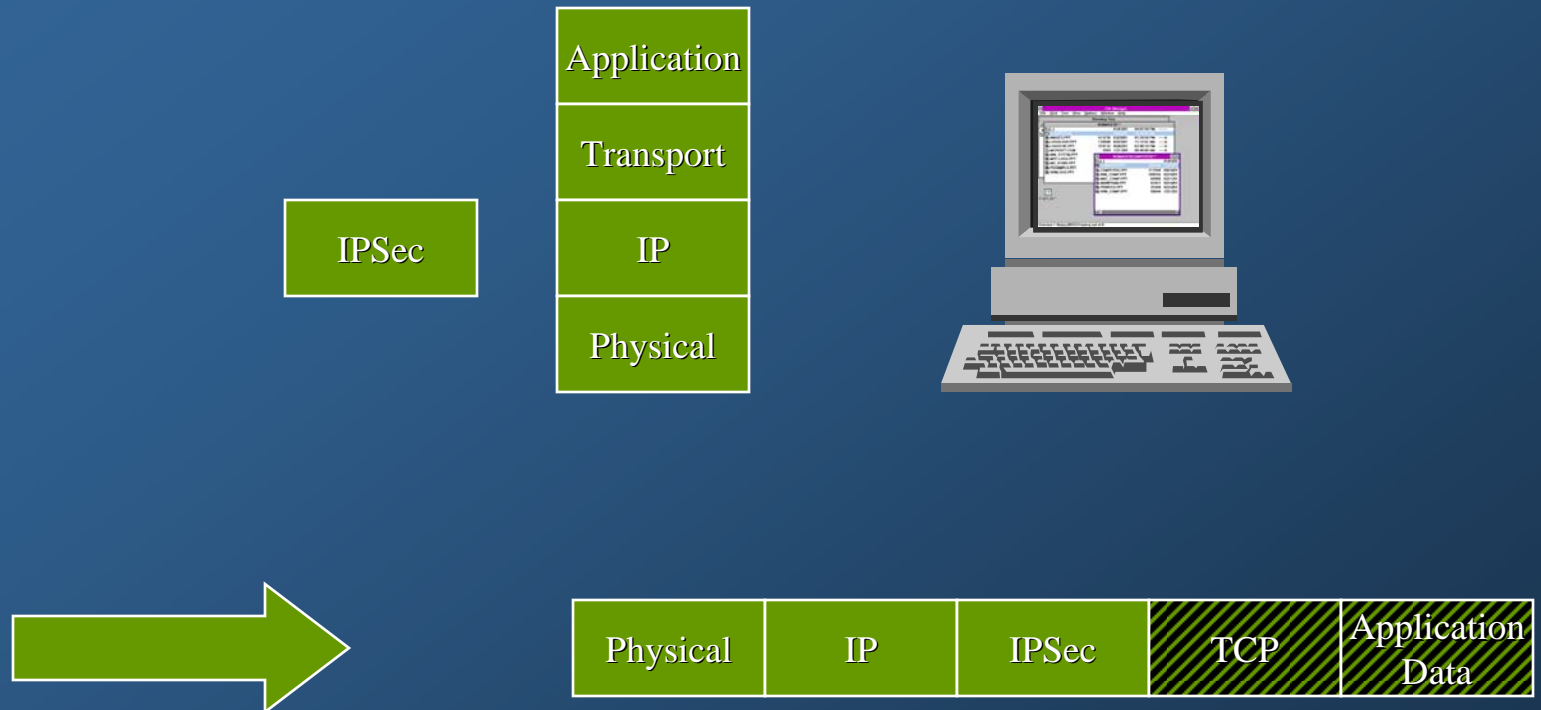
Sending in Tunnel Mode



Receiving in Tunnel Mode



Receiving in Transport Mode



Layer Two Tunneling Protocol (L2TP)

- Provides
 - Provides PPP encapsulation over IP
 - VPN services
- Doesn't Provide
 - A method of encryption for it's traffic
 - Protection against injection of packets into an open L2TP session

How L2TP Works

L2TP/IPSec



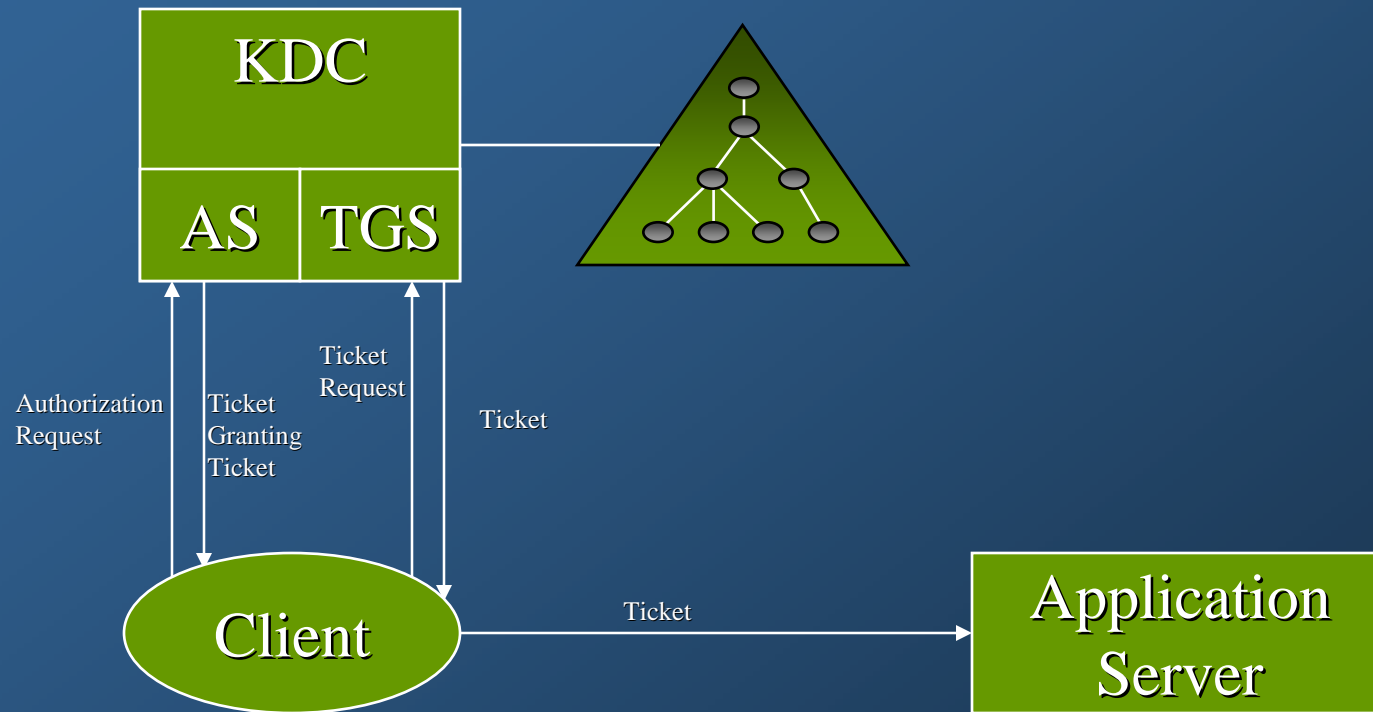
Kerberos

- Provides authentication of network server and client

What Kerberos Provides

- Mutual authentication of parties

How Kerberos Works



Public Key Infrastructure Basics

How Public Keys Are Used for Authentication

What's In a Certificate?

How PKI Works