KF School of Computing and Information Sciences
Florida International University

CNT 4403
Computing and Network Security

Network Security – IPSec

Dr. Kemal Akkaya

E-mail: *kakkaya@fiu.edu*

IPsec

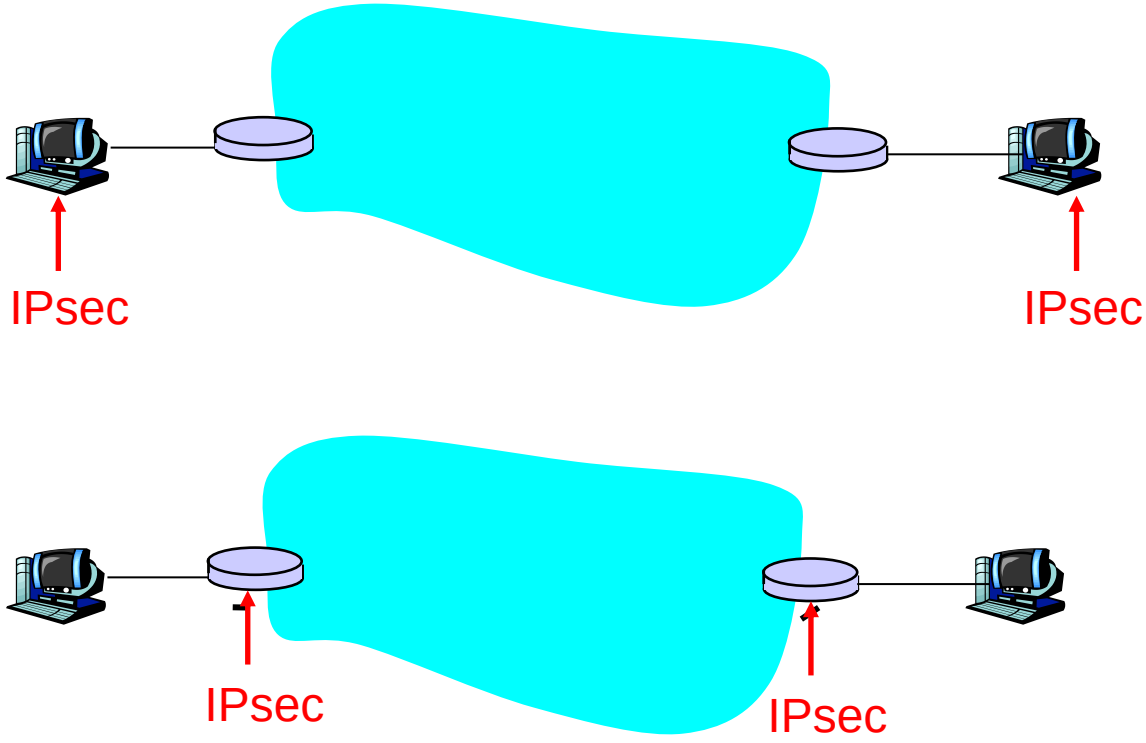
- **Cryptographic protection of the IP traffic**
- **IPsec sits "on top of" the network layer**
  - End-to-end or hop-by-hop security
  - Need to modify OS
  - All applications are "protected" by default, without requiring any change to applications or actions on behalf of users
  - Can only authenticate hosts, not users
  - User completely unaware that IPsec is running
- **Main components:**
  - Internet Key Exchange (IKE): IPsec key exchange protocol
  - Authentication Header (AH): Authentication of the IP packet (optional)
  - Encapsulating Security Payload (ESP): Encryption/authentication of the IP packet

Security Services Provided by IPSec

- **Authentication Header (AH) provides:**
  - Connectionless integrity
  - Data origin authentication
  - Protection against replay attacks
- **Encapsulating Security Payload (ESP) provides:**
  - Confidentiality (encryption)
  - Connectionless integrity
  - Data origin authentication
  - Protection against reply attacks
- **Both protocols may be used alone or applied in combination with each other.**

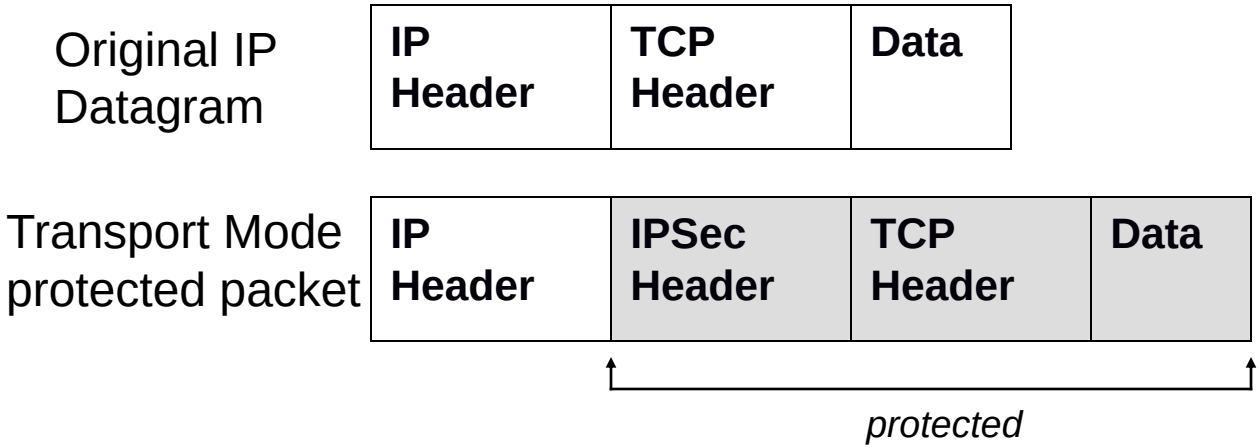
Uses of IPsec

- **Protocol modes:**
  - Transport mode: Host applies IPsec to transport layer packet
  - Tunnel mode: Gateway applies IPsec to the IP packet of a host from the network (IP in IP tunnel)
- **Typical uses:**
  - Remote access to network (host-to-gateway)
  - Virtual private networks (VPN) (gateway-to-gateway)

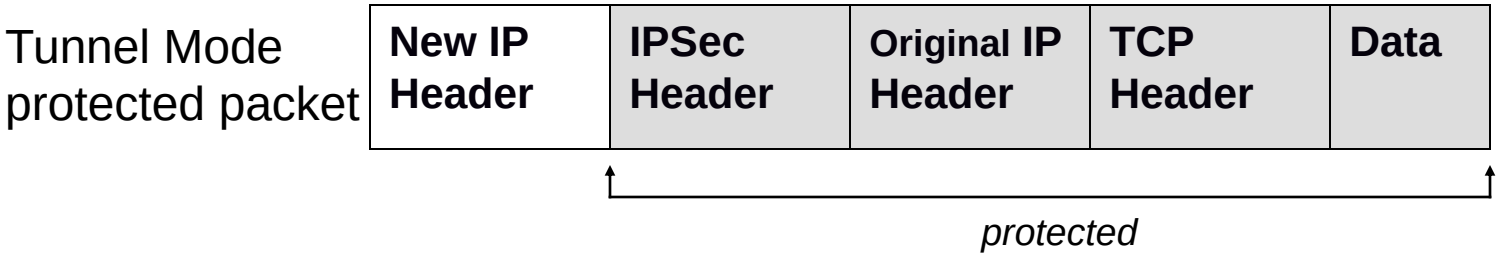


IPSec Modes of Operation

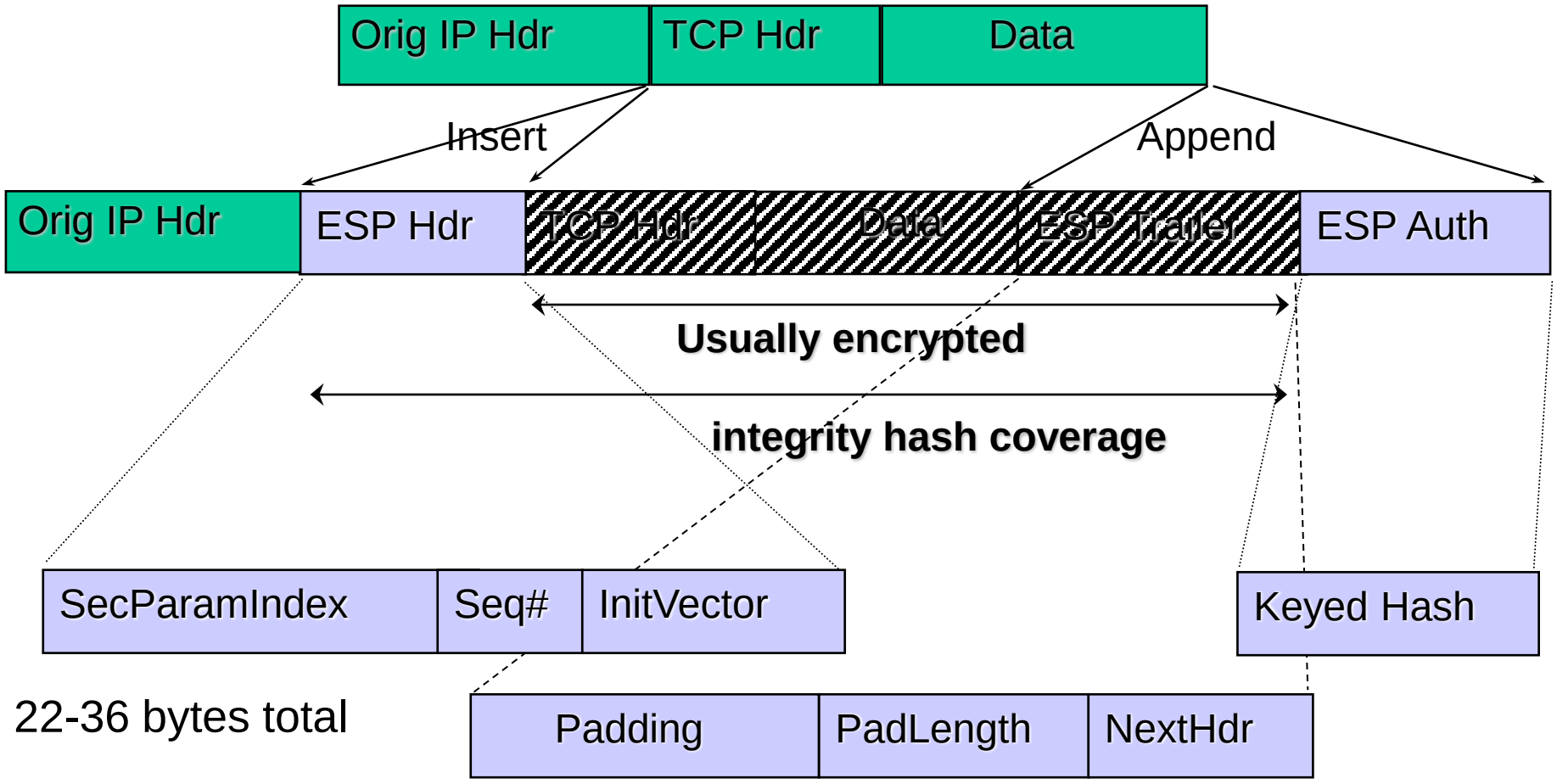
❑ Transport Mode: protects the upper layer protocols



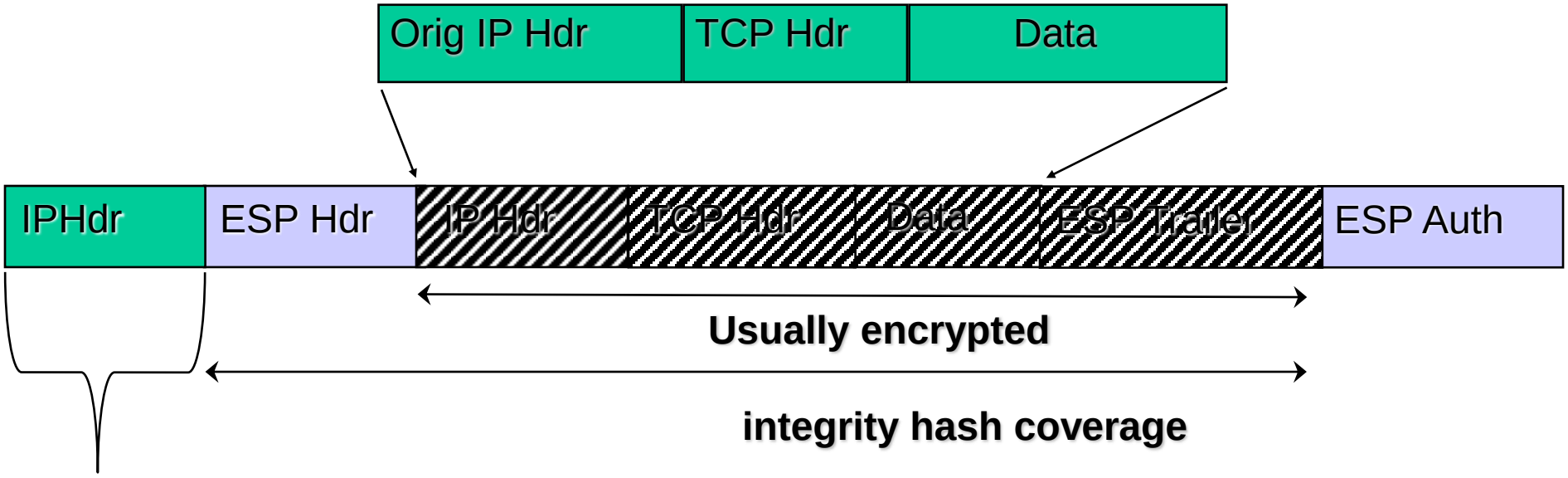
❑ Tunnel Mode: protects the entire IP payload



Encapsulating Security Payload (ESP) in Transport Mode

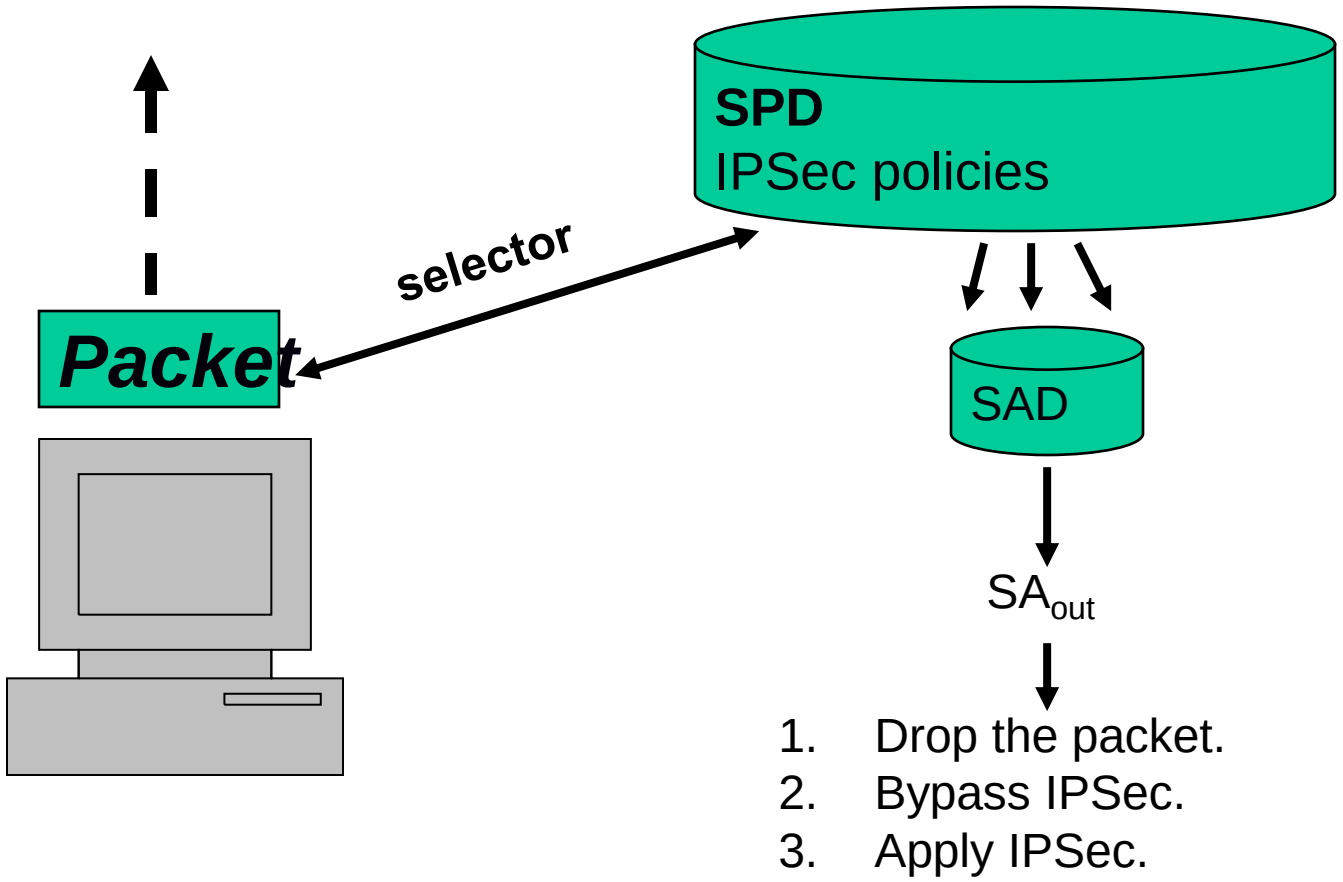


IPSec ESP Tunnel Mode



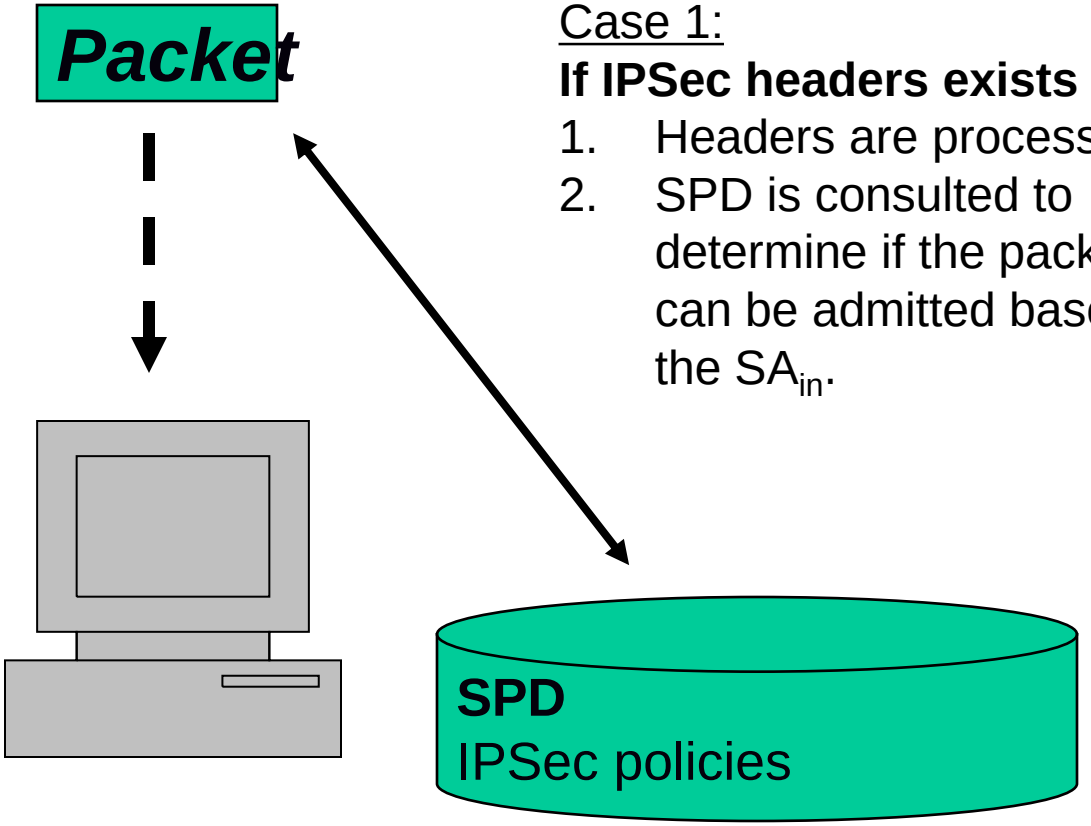
Transport Mode Header for comparison

Outbound IPSec Processing



SPD = Security Policy Database: *Find what to do with the packet in linear search*
SAD = Security Association Database: *How to do based on SecParamIndex (SPI)*
SA = Security Association

Inbound IPSec Processing



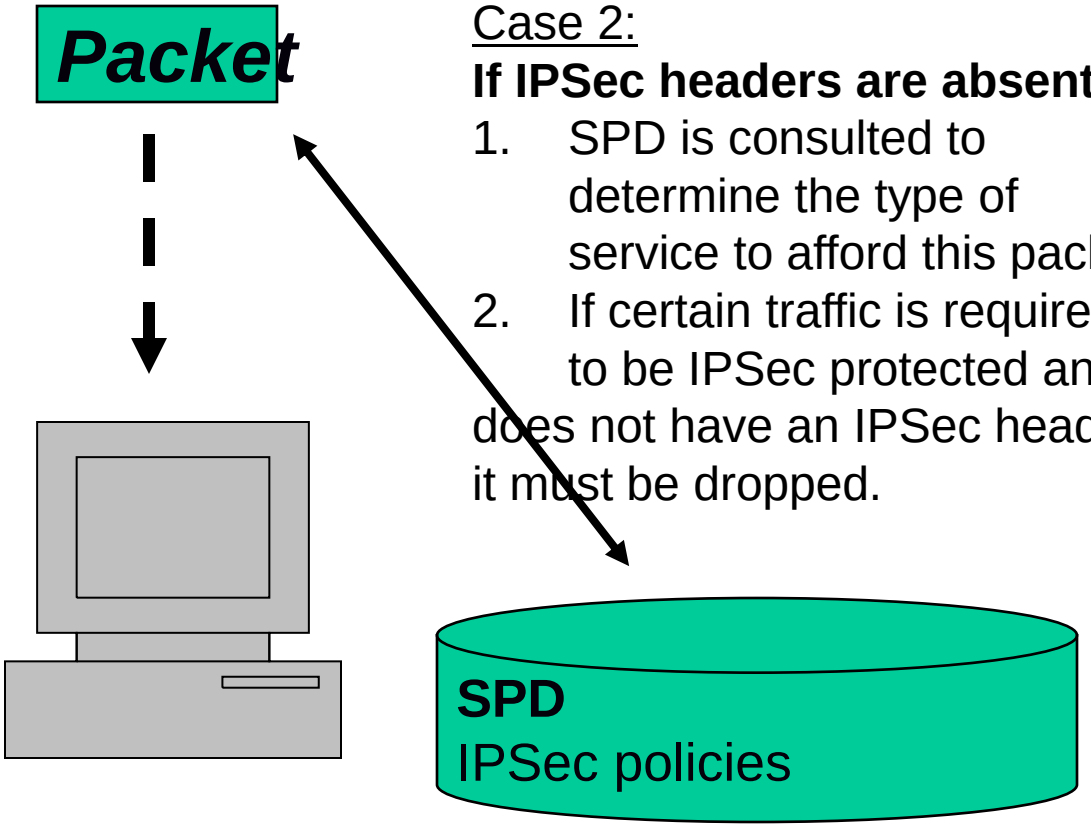
Case 1:

If IPSec headers exists

1. Headers are processed.
2. SPD is consulted to determine if the packet can be admitted based on the SA_{in}.

SPD = Security Policy Database
SAD = Security Association Database
SA = Security Association

Inbound IPSec Processing



Case 2:

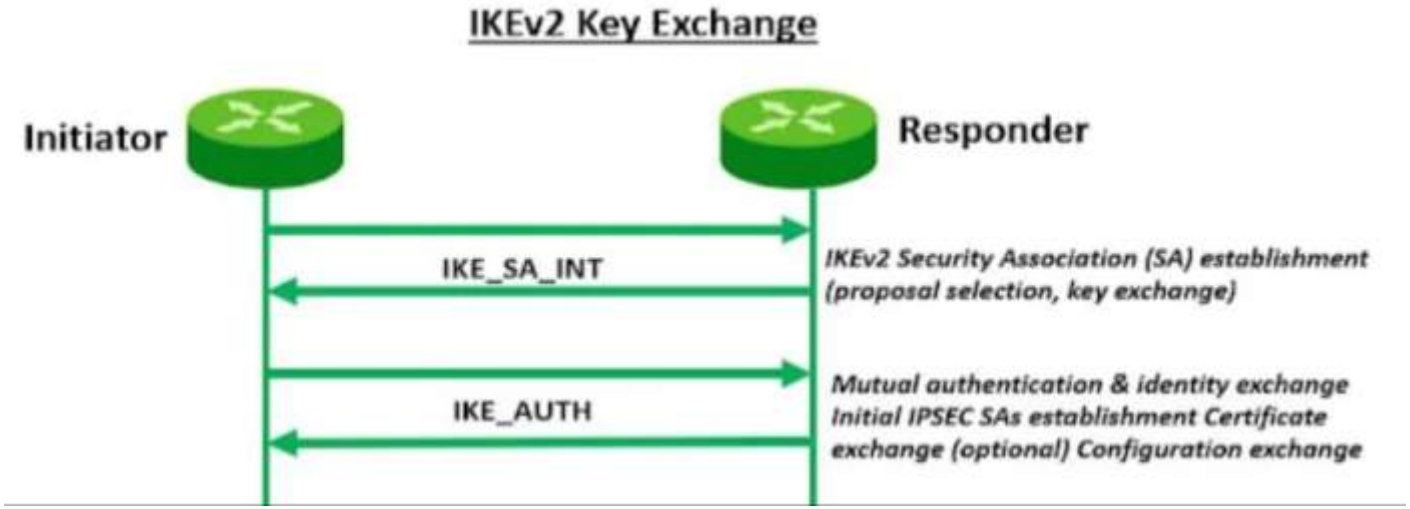
If IPSec headers are absent

1. SPD is consulted to determine the type of service to afford this packet.
2. If certain traffic is required to be IPSec protected and the packet does not have an IPSec header, it must be dropped.

SPD = Security Policy Database
SAD = Security Association Database
SA = Security Association

Key Management in IPSec

- ESP require encryption and authentication keys
- Process to negotiate and establish IPSec keys between two entities
- IKE (Internet Key Exchange):
  - Consists of ISAKMP and Oakley.
    - ✓A variant of Diffie-Hellman
  - IKEv1 and IKEv2 exist



IPSec Advantages

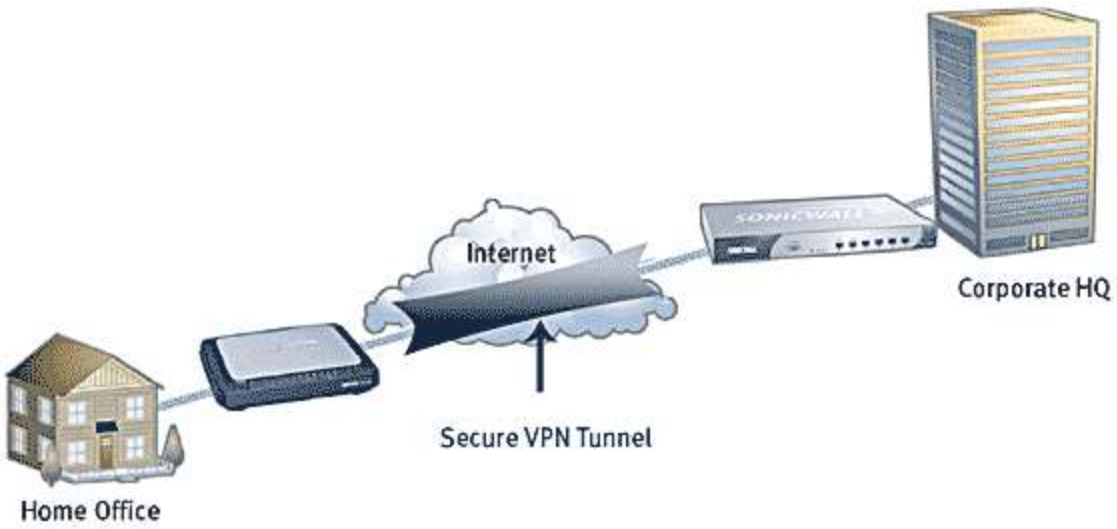
- **Does not mandate PKI (for authentication: pre-shared key can be used instead) and comes with IPv6**
- **Since it runs at Layer 3, will protect any transport or application on top of Layer 3.**
  - This would allow us to secure both any transport protocol or any application (i.e. it's application independent)
- **Transparent to applications as it is integrated into the kernel**
  - Transparent enough that it can be used with many key management protocols (manual keying, IKEv1, IKEv2)
- **Supports multiple modes (transport or tunnel).**
  - Transport mode is used for secure sessions between end devices where tunnel mode is used between security gateways.
  - Tunnel mode adds an extra layer of security as both the header and payload are encrypted (in transport mode, only the payload is encrypted)
- **VPNs use IPSec**
  - For example, used in Cisco PIX firewall, many remote access gateways
- **Can be used with Kerberos Authentication System (MIT)**

IPSec Disadvantages

- **In IETF, TLS is preferred to IPsec**
- **Since it is embedded within the IP stack, it would require kernel level changes**
- **At best, provides data-origin authentication.**
  - This is network to network authentication.
  - You are not authenticating a particular user but anyone that could be using that device
- **Configuring IPsec and IKE is complex and cumbersome**
  - IPSec has been out for 20 years (IPv6 deployment), but wide deployment has been hindered by complexity
- **With an IPsec VPN, it does not allow for application filtering.**
  - You have access to the full network (i.e. you are part of the corporate network)
- **IPsec is not NAT friendly**

Virtual Private Networks (VPNs)

- **Private and secure network connection between systems**
  - Uses data communication capability of unsecured and public network
- **Securely extends organization's internal network connections to remote locations beyond trusted network**
- **Avoid leased lines**
  - Thus cost effective



VPN Implementations

- **Three VPN technologies defined:**
  - Trusted VPN
  - Secure VPN
  - Hybrid VPN (combines trusted and secure)
- **A trusted VPN, or VPN, uses leased circuits from a service provider and conducts packet switching over these leased circuits.**
- **Secure VPNs use security protocols and encrypt traffic transmitted across unsecured public networks like the Internet.**
  - We focus on this one
- **A hybrid VPN combines the two, providing encrypted transmissions (as in secure VPN) over some or all of a trusted VPN network.**

Secure VPN Provides…

- ***Encapsulation or Tunneling*** **of incoming and outgoing data**
  - the native protocol of the client is embedded within the frames of a protocol that can be routed over the public network, as well as be usable by the server network environment.
    - ✓ Encapsulation vs Tunneling
- ***Encryption*** **of incoming and outgoing data**
  - keep the data contents private while in transit over the public network but usable by the client and server computers and/or the local networks on both ends of the VPN connection.
- ***Authentication*** **of the remote computer and, perhaps, the remote user as well.**
  - Authentication and the subsequent authorization of the user to perform specific actions are predicated on accurate and reliable identification of the remote system and/or user.

Secure VPN Implementation Options

- **The protocols they use to tunnel the traffic**
  - E.g., IPSec, SSL
- **The tunnel's termination point**
  - Customer edge
  - Network provider edge
- **Whether they offer site-to-site or remote access connectivity**
  - ATM/Frame Relay - Trusted VPN
  - Internet Remote Access – Secure VPN
- **The levels of security provided**
- **The OSI Layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity**
  - Layer 2 – PPP
  - Layer 3 - IPSec

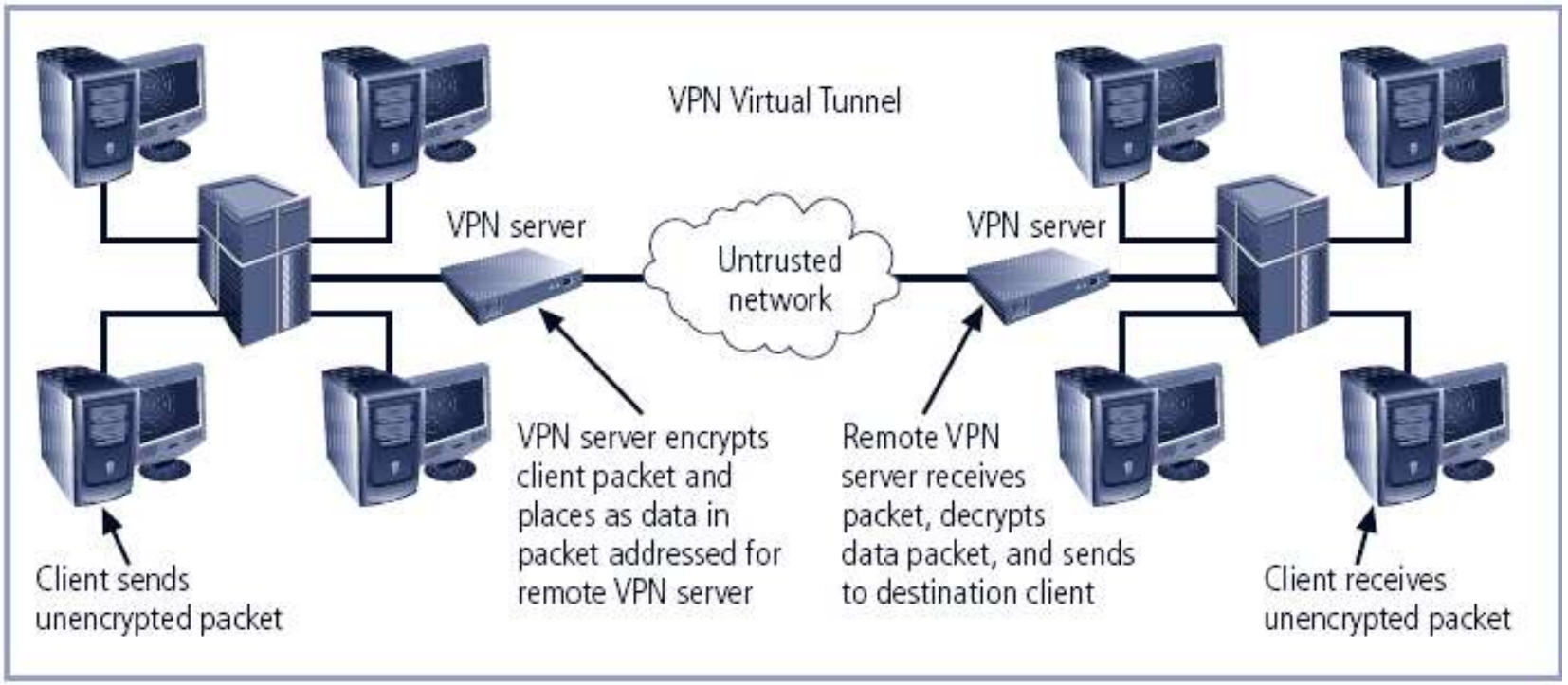


FIGURE 6-19 Tunnel Mode VPN

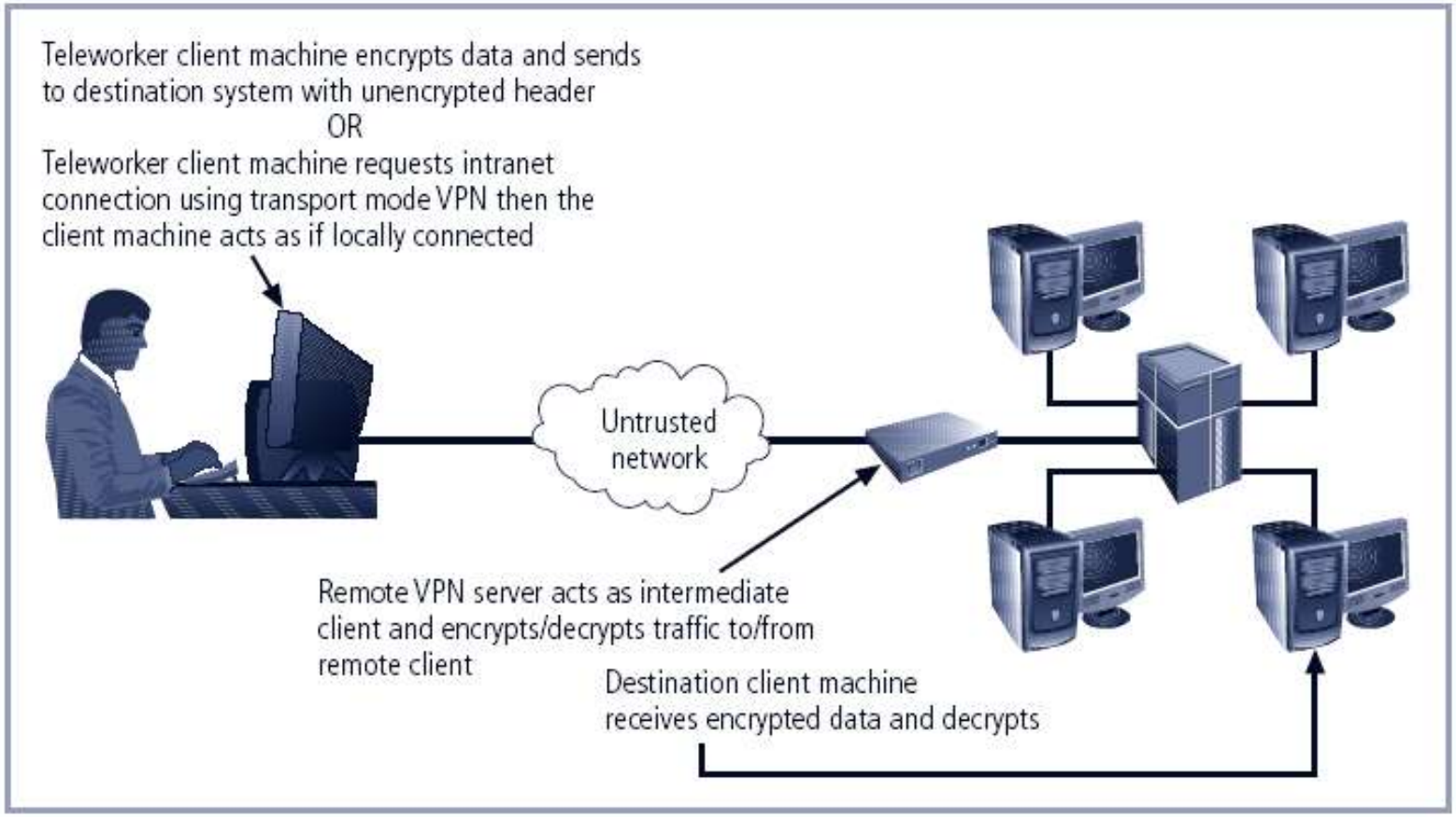


FIGURE 6-18 Transport Mode VPN

Pros and Cons

- **VPN Advantages**
  - Cost Effective
  - Greater scalability
  - Easy to add/remove users
  - Mobility
  - Security
- **VPN Disadvantages**
  - Unpredictable Internet traffic
  - Difficult to accommodate products from different vendors