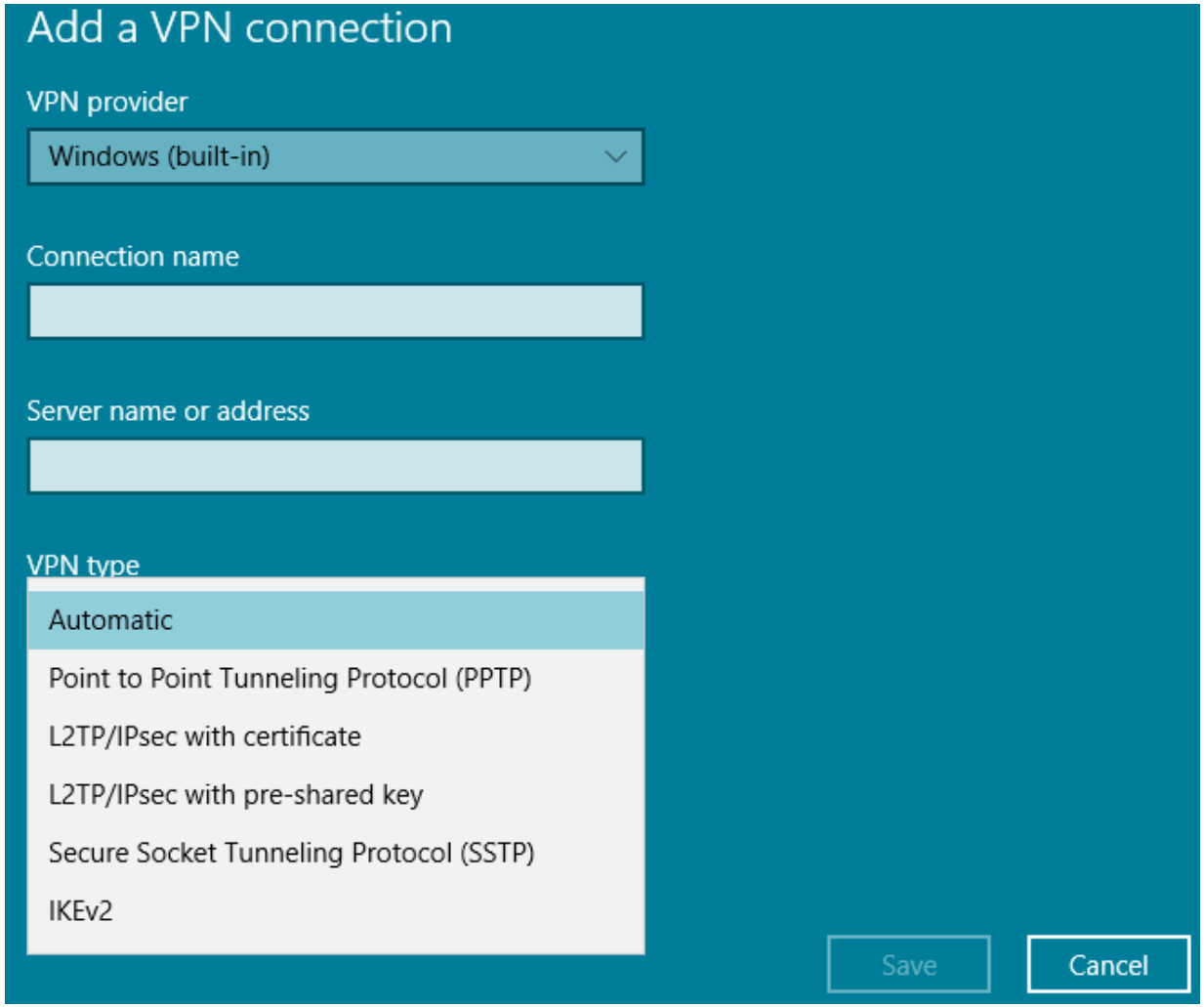
IPSec

- Internet Protocol Security (IPSec) is a framework consisting of protocols and algorithms for protecting data through an un-trusted network such as Internet.

- Why do we need IPsec?
  - Because the IP protocol itself doesn't have any security features at all. IPsec is a complex framework consisting of many settings, which is why it provides a powerful and flexible set of security features that can be used. The main reason that IPSec is so powerful is that it provides security to IP, the basis for all other TCP/IP protocols. In protecting IP, we are protecting pretty much everything else in TCP/IP as well.
  - Many VPNs use the IPsec protocol suite to establish and run these encrypted connections. However, not all VPNs use IPsec. Another protocol for VPNs is SSL/TLS, which operates at a different layer in the OSI model than IPsec.

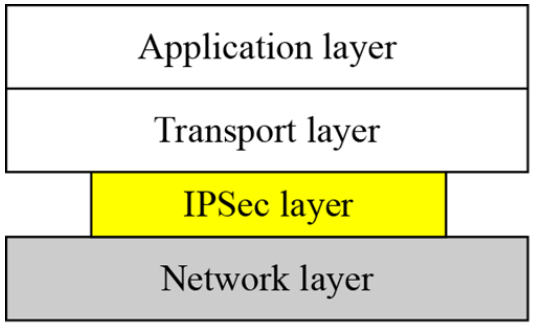
- IPsec is mandatory in IPv6 and can be used with IPv4 too.

IPSec cont…

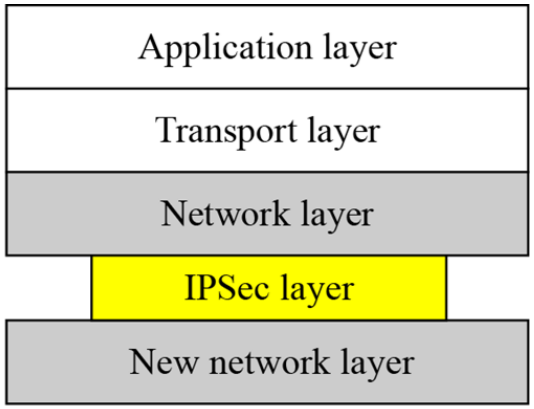

Add a VPN connection
VPN provider
Windows (built-in)
Connection name
Server name or address
VPN type
Automatic
Point to Point Tunneling Protocol (PPTP)
L2TP/IPsec with certificate
L2TP/IPsec with pre-shared key
Secure Socket Tunneling Protocol (SSTP)
IKEv2
Save
Cancel

IPsec location

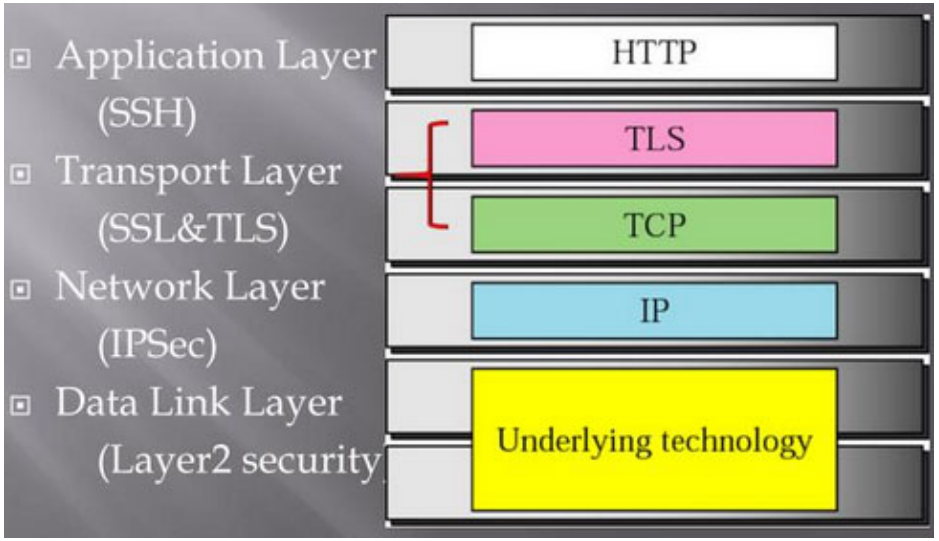
- IPsec designed to provide security at layer 3 (IP) below layer 4 (TCP or UDP).



Transport Mode

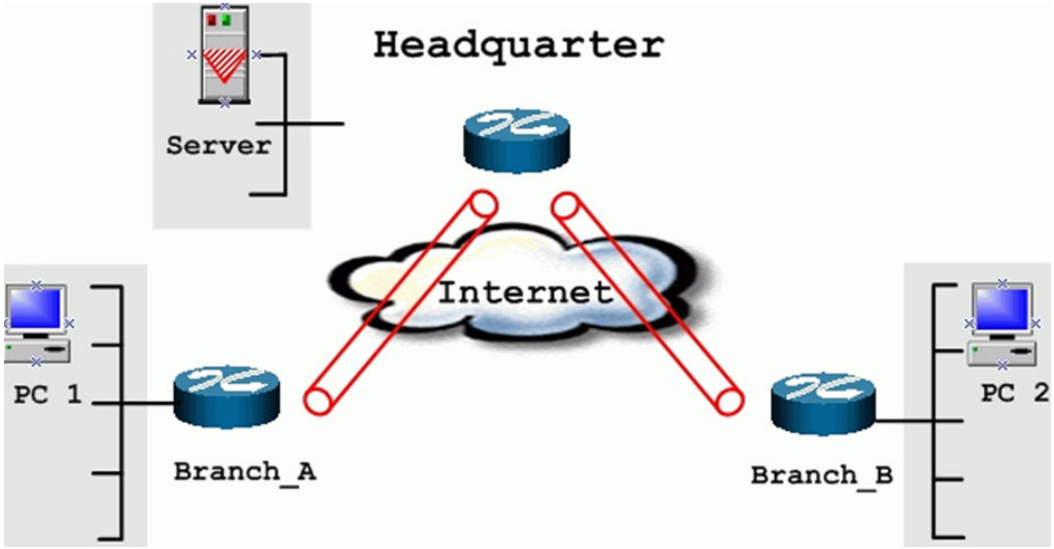


Tunnel Mode

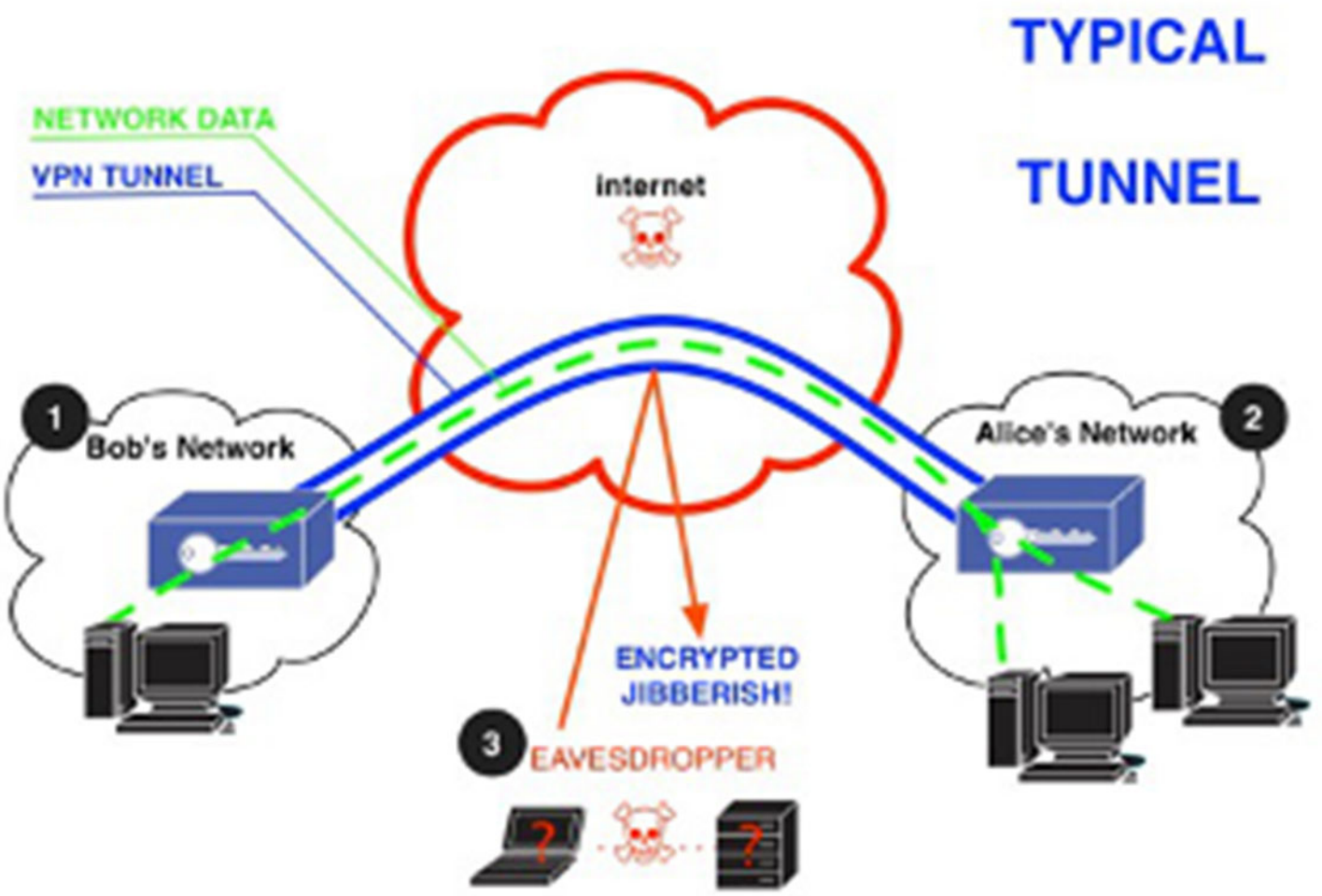


IPsec cont…

- Ideally, any institution would want its own private network for communication to ensure security. However, it may be very costly to establish and maintain such private network over geographically dispersed area. It would require to manage complex infrastructure of communication links, routers, DNS, etc.
- IPsec provides an easy mechanism for implementing Virtual Private Network (VPN) for such institutions. VPN technology allows institution's inter-office traffic to be sent over public Internet by encrypting traffic before entering the public Internet and logically separating it from other traffic.



IPsec cont…


TYPICAL
TUNNEL
NETWORK DATA
VPN TUNNEL
Internet
1
Bob's Network
2
Alice's Network
ENCRYPTED
JIBBERISH!
3
EAVESDROPPER

IPsec services

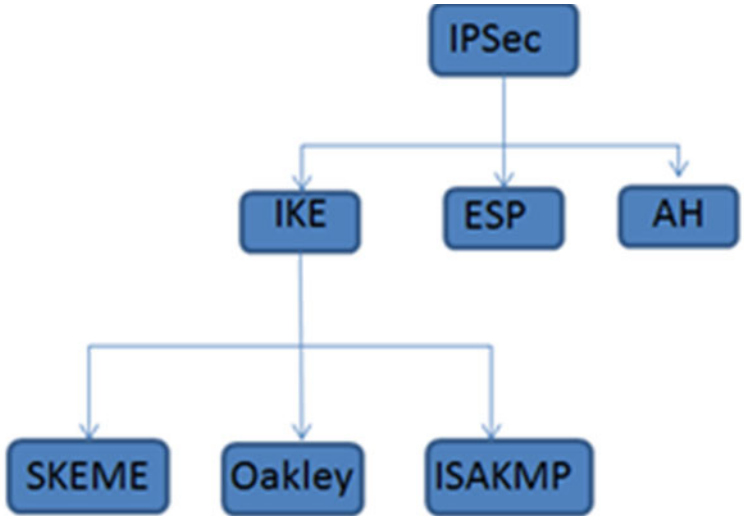
- IPsec, as a framework, can protect our traffic with the following security services:
  - Confidentiality/Privacy: by encrypting our data, nobody except the sender and receiver will be able to read our data.
  - Authentication: the sender and receiver will authenticate each other by for example certificates to make sure that we are really talking with the device we intend to.
  - Integrity: we want to make sure that nobody changes the data in our packets. By calculating a hash value, the sender and receiver will be able to check if changes have been made to the packet.
  - Anti-replay: even if a packet is encrypted and authenticated, an attacker could try to capture these packets and send them again. By using sequence numbers, IPsec will not transmit any duplicate packets which causes duplicate packets to be dropped.

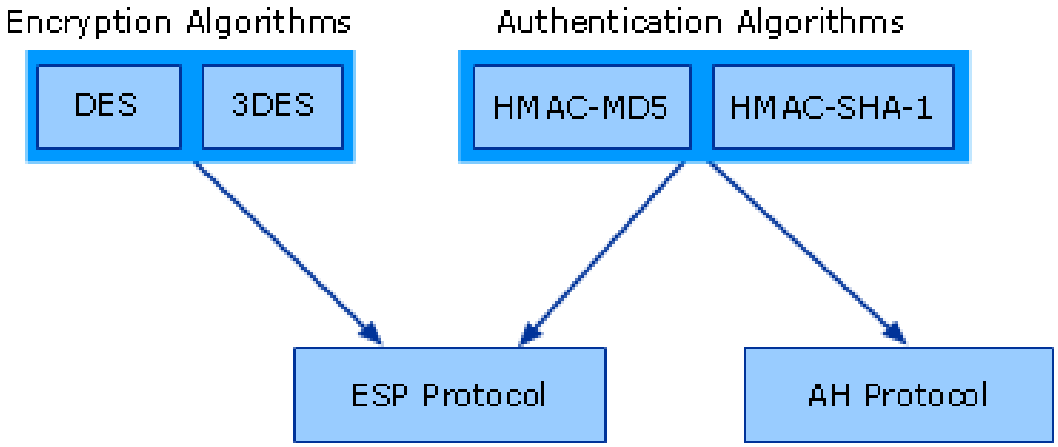
IPsec protocols

- To implement these services, IPsec as a framework, uses a variety of protocols.
- The main components of IPSec include:
  - Authentication Header (AH): provides source authentication, integrity, and anti-replay protection but *not* confidentiality
  - Encapsulating Security Payload (ESP): provides source authentication, integrity, anti-replay, and confidentiality. It is more widely used than AH
  - Internet key exchange (IKE): for negotiating security parameters & establishing authentication keys (security association)

Services	*AH*	*ESP*
Access control	Yes	Yes
Message authentication (message integrity)	Yes	Yes
Entity authentication (data source authentication)	Yes	Yes
Confidentiality	No	Yes
Replay attack protection	Yes	Yes

IPsec protocols cont…

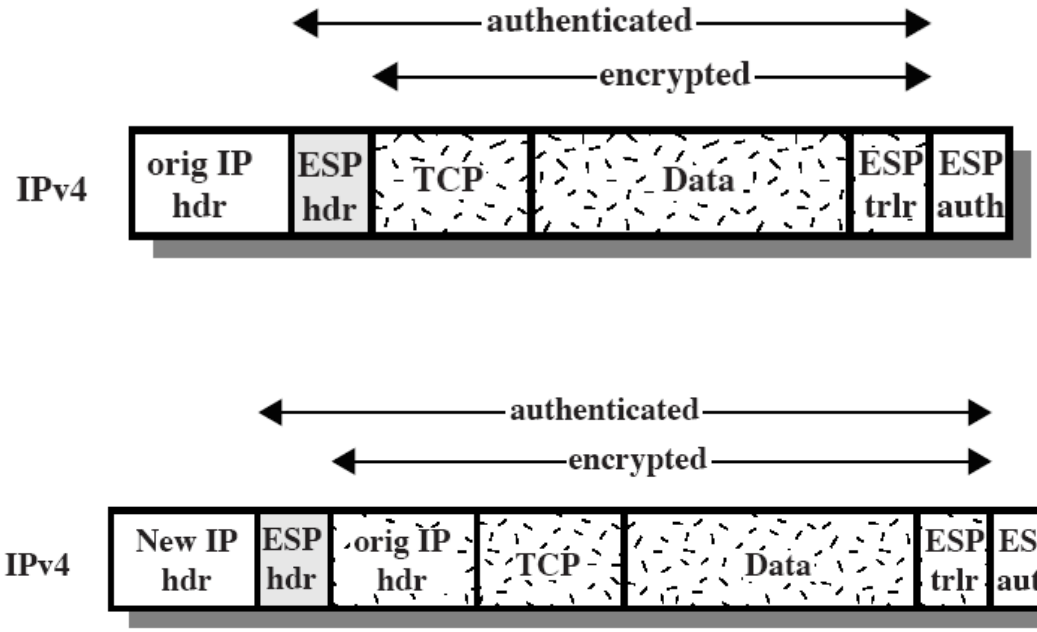




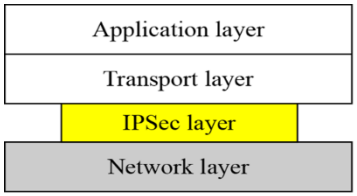
IPsec modes

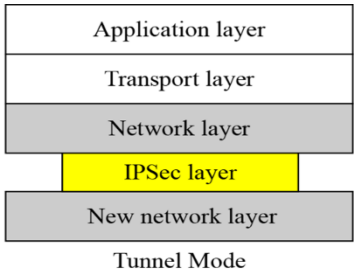
- An IPsec mode describes how the original IP packet is transformed into a protected packet.

- Both ESP and AH can work in two different protection modes:
  - Transport mode: it is the default mode
  - Tunnel mode

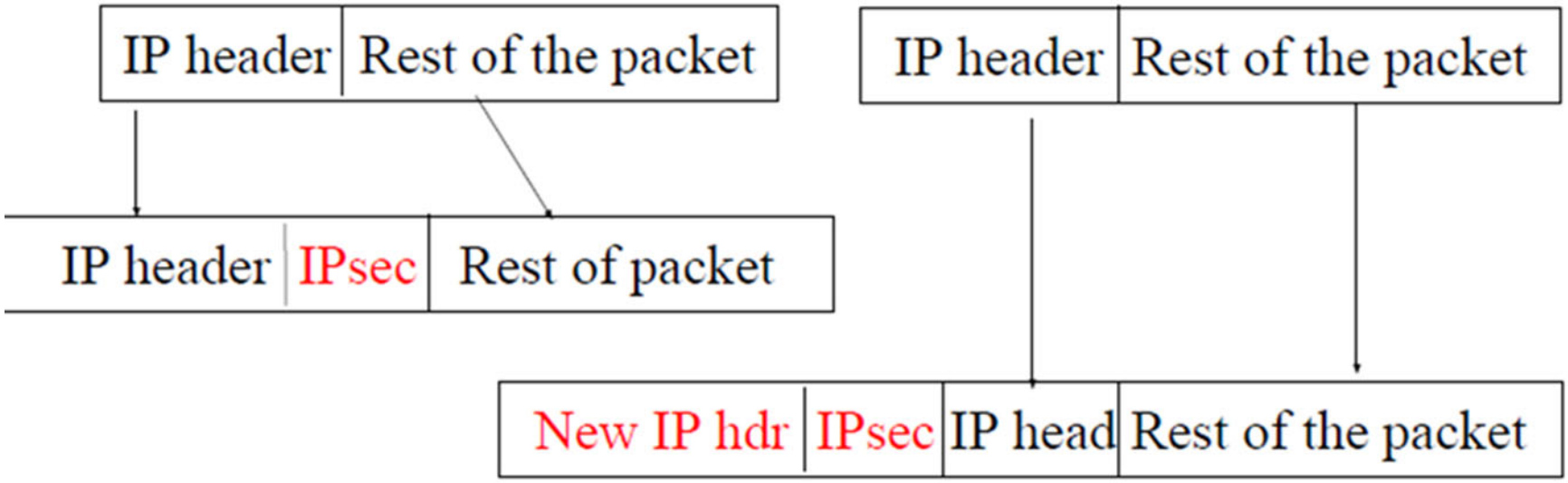


IPsec modes cont…





- Transport mode encapsulates only the transport layer information within the IPsec protection.
- Tunnel mode encapsulates the entire IP packet along with its headers and then generates a new header to stick on top of the encrypted ip packet.



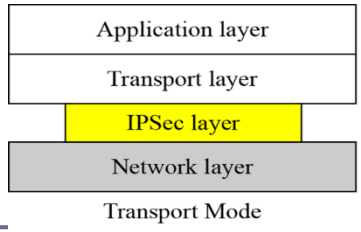
IPsec modes cont…

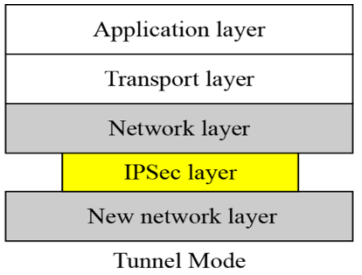
- Thus, four combinations are possible:

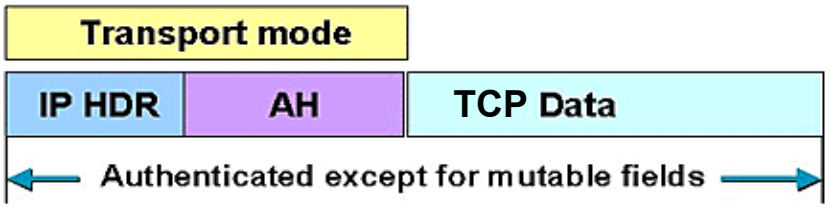
Transport mode with AH	Transport mode with ESP
Tunnel mode with AH	Tunnel mode with ESP

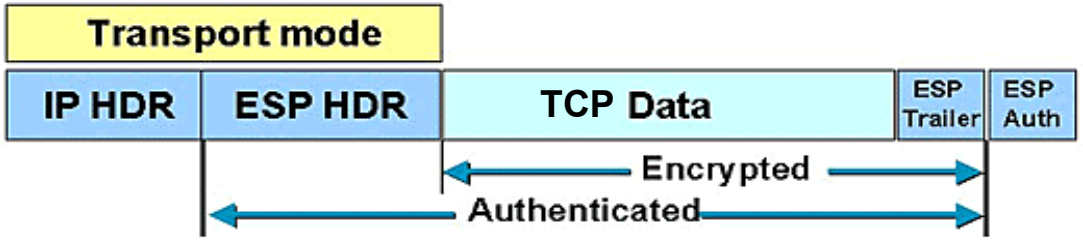
Most common and most important

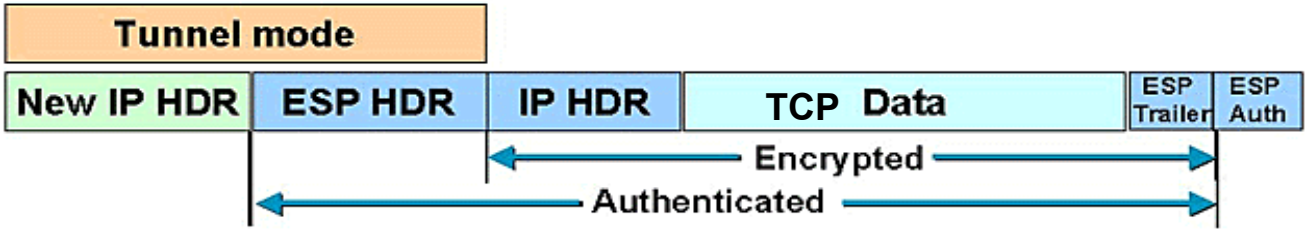
IPsec modes cont…







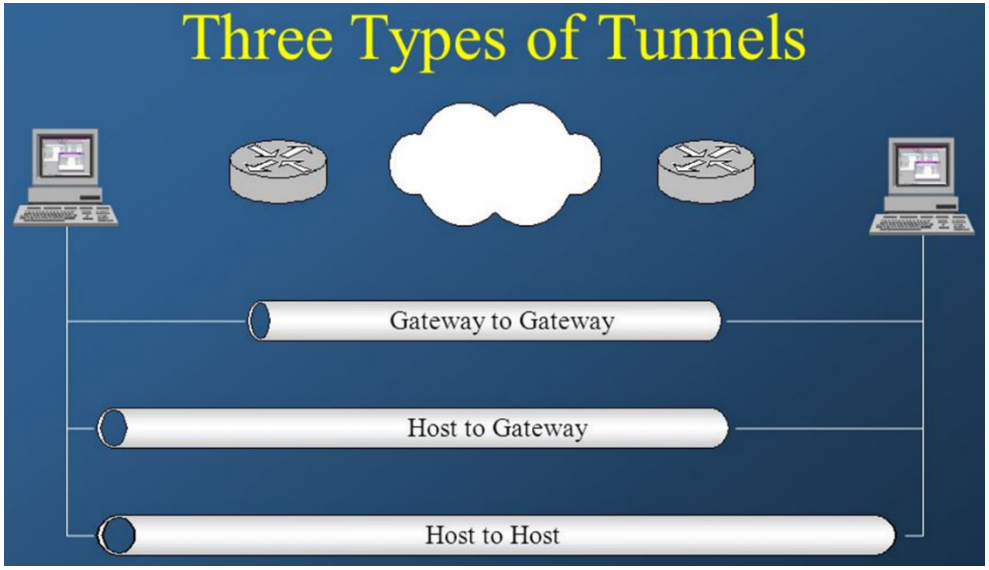




IPsec modes cont…

- Transport mode is used when both the cryptographic endpoints are also the communication endpoints of the secured IP packets:
- Tunnel mode is used when at least one cryptographic endpoint is not a communication endpoint of the secured IP packets.

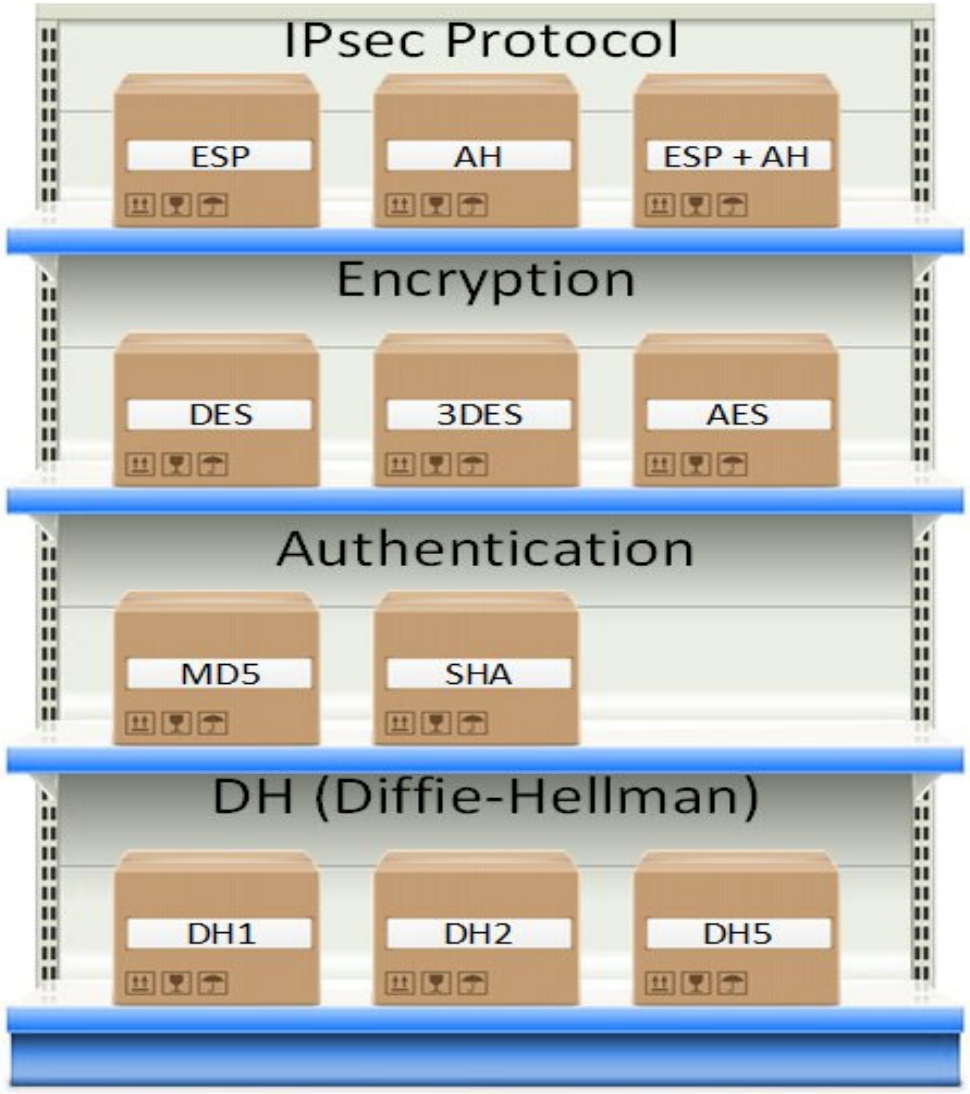
  - Cryptographic endpoints: the entities that generate/process an IPSec header (AH or ESP)
  - Communication endpoints: Source and Destination of an IP packet.



IPsec security

- Each IPsec connection can provide different security services such as encryption, integrity, authenticity.
- And as we mentioned, there are many different security algorithms that the IPsec peers can select to protect the transmitted data.
- When the security service is determined, the two IPsec peers must determine different parameters such as which protocol (AH, ESP) to use, which algorithm to use (for example, DES or 3DES for encryption; MD5 or SHA-1 for integrity), etc.
- After deciding on the parameters, the two devices must share session keys.
- IPsec transform= protocol + algorithm. For example, AH with HMAC-MD5.

IPsec security cont…



IPsec security cont…

- Therefore, as we can see, there are many information to manage.
- Thus, the source and destination peers have to go through some negotiations to exchange their supported security parameters and then agree on which security services and security protocols with which mode they select to be used during the IPsec session to protect data.

IPsec databases

- IPsec has two entities that control what happens to a packet:
  - security policy (SP): what to do. Security policies for a device are stored in the device's security policy database (SPD).
  - security association database (SA): how to do it. A device's security associations are contained in its security association database (SAD).

SP

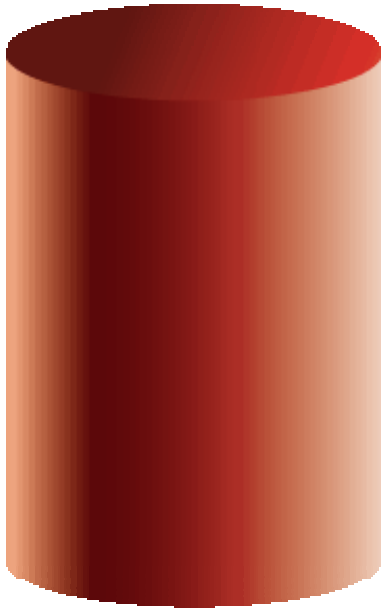
- Security Policies ==> "General guidelines". It tells you what to do: decide whether to run for IPsec, use or not AH, ESP, etc. You analyze all available options.
- A security policy is a rule that is programmed into the IPSec implementation that tells it what to do to process different datagrams received by the device. For example, security policies are used to decide if a particular packet needs to be processed by IPSec or not; those that do not bypass AH and ESP entirely. If security is required, the security policy provides general guidelines for how it should be provided, and if necessary, links to more specific detail.

SA

- Security Association ==> "Particular type of secure connection". A Security Association (SA) is a set of security information that describes a particular kind of secure connection between one device and another. You can consider it a "contract“ that specifies the particular security mechanisms that are used for secure communications between the two.

SP cont…

- Each policy entry in the SPD includes:
  - Selectors (a set of fields of the IP packet)
    - Source and Destination IP Address
    - Source and Destination Ports
    - Transport Layer Protocol
    - Name
  - The policy :
    - Discard the packet, bypass or process IPSec
    - For IPSec Processing :
      - Security Protocol and Mode
      - Enabled Services (anti-replay, authentication, encryption)
      - Algorithms (for authentication and/or encryption)
  - Pointer to an active SA in the SAD (if it exists)



SPD

SP cont…

- While the SPI is provided to map the incoming packet to an SA in SAD, the IP traffic is mapped to IPSec policies by selectors in SPD.
- Each policy is associated with one or more selectors.
- Each entry in the SPD is indexed by the selector and specifies one of the following three actions/security policies to be performed for an IP packet if it matches the selector:
  - Discard/Drop: do not let this packet in or out
  - Protect: process by the IPSec module, in which case the SPD entry points to an SA:
    - Outbound: apply security
    - Inbound: check that security has been applied
  - Bypass: pass the packet to the IP stack for normal forwarding:
    - Outbound: do not apply IPsec on this packet
    - Inbound: do not expect IPsec on this packet

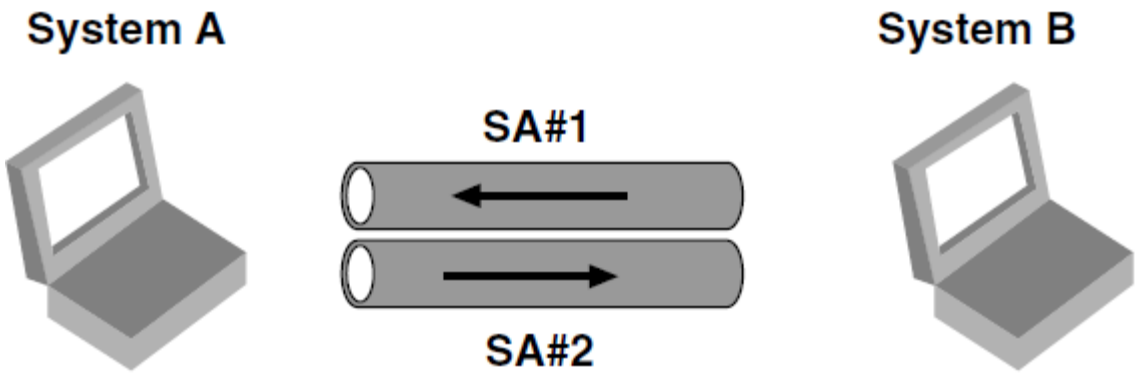
SP cont…

- Host SPD example

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP in transport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP in transport-mode	Encrypt to server
TCP	1.2.3.101	≥1024	1.2.4.10	443	BYPASS	Allow TLS, no double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

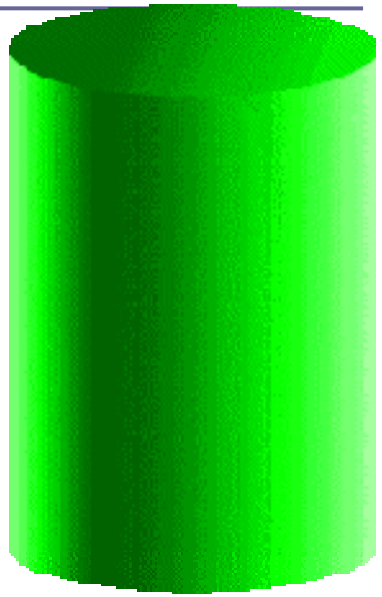
SA cont…

- A security association (SA) is the collection of security algorithms and parameters that the two communicating hosts agree to use.
- SA is a unidirectional/simplex logical connection between two IPSec systems.
- Thus, two SAs are required for a bi-directional communication, a single SA protects data in one direction (inbound or outbound).
  - The outgoing packet has an associated SA that applies to it.
  - The incoming packet is assigned an SA to understand how to handle the data being received.



SA cont…

- Each SA entry in the SAD includes:
  - Identifier:
    - SPI (carried in AH or ESP headers)
    - Destination IP address
    - IPsec Protocol
  - Parameters:
    - IPsec transform
      - Security Protocol Mode (tunnel or transport)
      - Encryption algorithm and keys
      - Authentication algorithm and keys
      - Anti-replay service (sequence counters)
    - Key lifetime
    - SA lifetime (when this lifetime expires, the SA must be terminated, and a new SA established)
    - Link with an associated policy in the SPD
    - Some extra parameters such as path MTU



SA cont…

- The Security Parameter Index (SPI) shows which entry (SA) in SAD.
- SPI is provided to map the packet to an SA in SAD.
- The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed/handled.
- The SPI has local significance only.

SPI is sent with packet, tells recipient which SA to use.

SPD indicate what to do with the packet.
SAD indicates how to do it.

SPD/SAD example

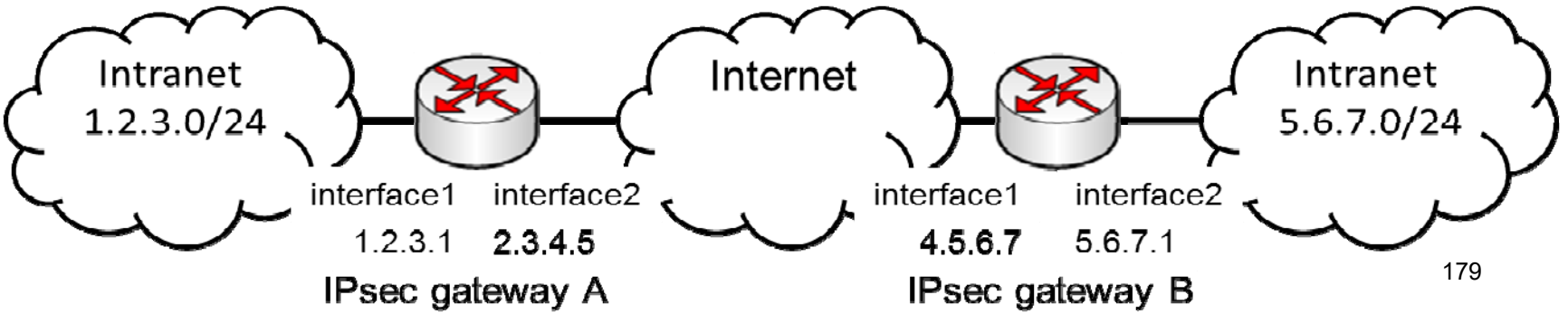
SPD of gateway A, interface 2

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	2.3.4.5	500	4.5.6.7	500	BYPASS	IKE
*	1.2.3.0/24	*	5.6.7.0/24	*	ESP tunnel to 4.5.6.7	Protect VPN traffic
*	*	*	*	*	BYPASS	All other peers

Pointers to created associations

SAD of gateway A

SPI	SPD selector values	Protocol	Algorithms, keys, algorithm state
spi1	TCP, 1.2.3.0/24, 5.6.7.0/24	ESP tunnel from 4.5.6.7	…
spi2	–	ESP tunnel to 4.5.6.7	…

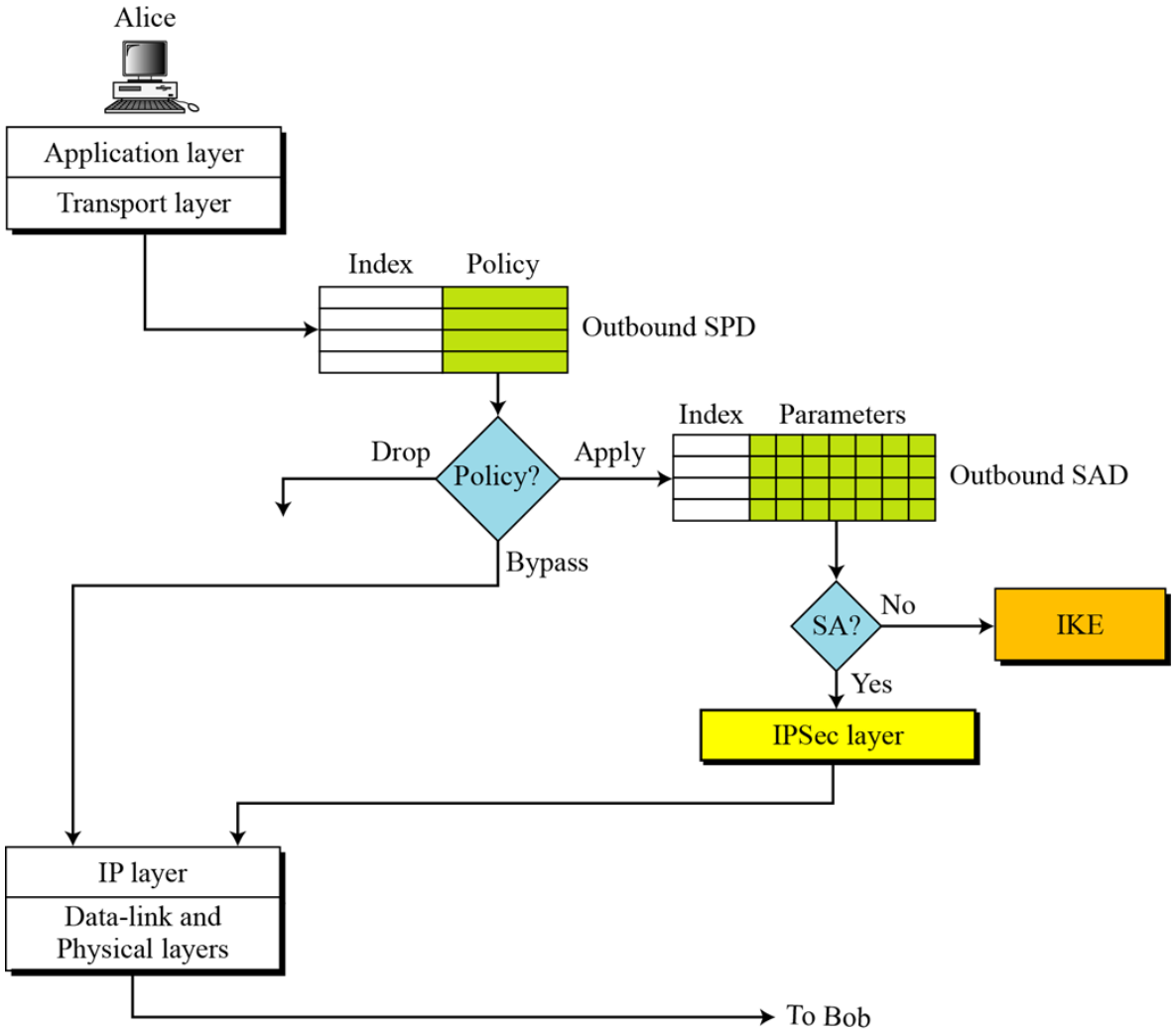


Packet processing by IPsec

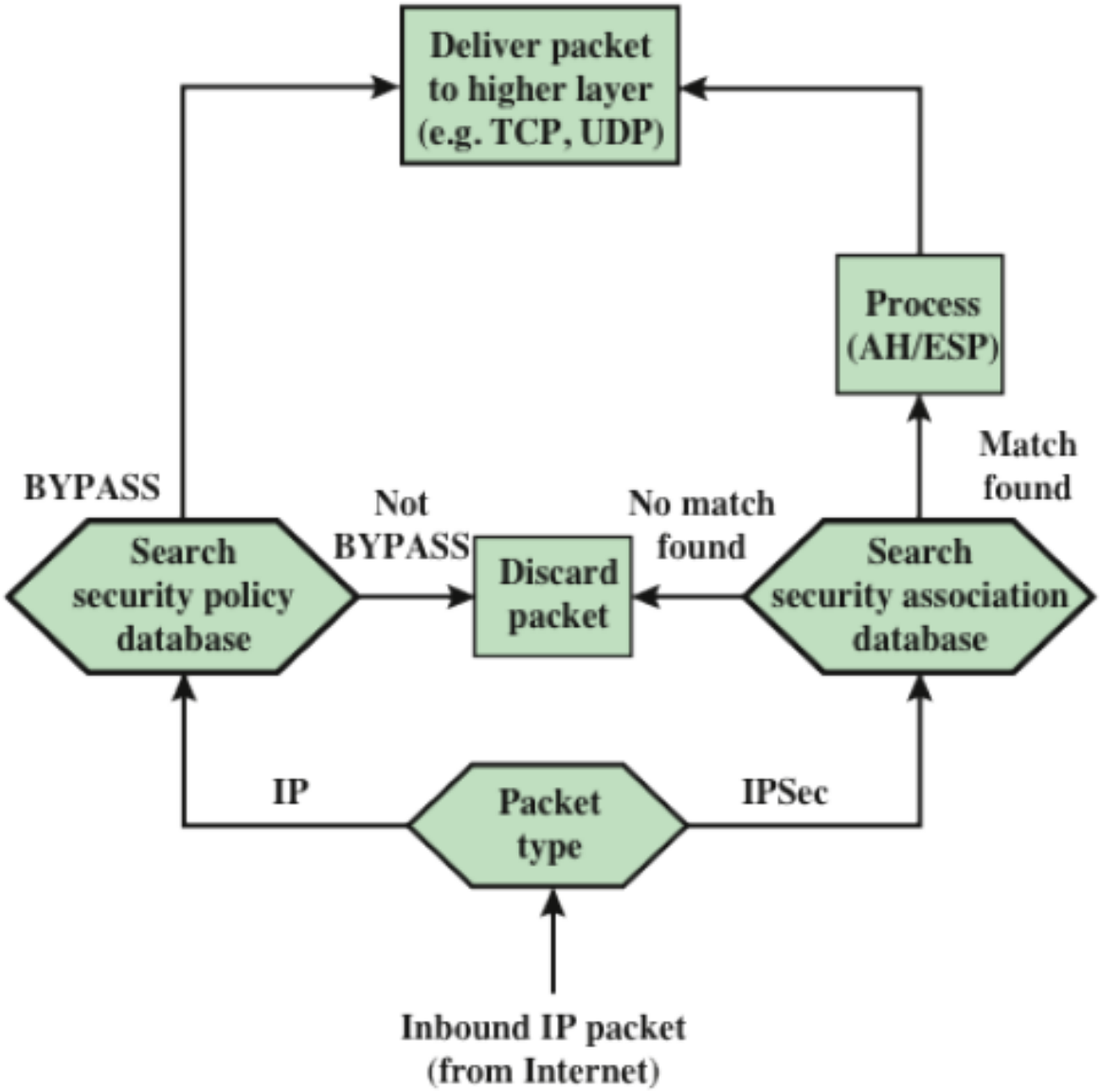
- Processing of packets in IPsec:
  - outbound/outgoing
  - inbound/incoming

Outbound packet processing cont…

- Before an IP packet is passed to the link layer, a lookup in the SPD is performed to check whether to secure the packet with IPSec or not.
- If the SPD has no policy, the packet is send without IPSec protection.
- If at least one policy in the SPD is found, the SA or SAs in the SAD associated with the policy, are applied on the packet to protect it and the SPI is inserted into the IPSec packet so that the receiver can process the IPSec packet.

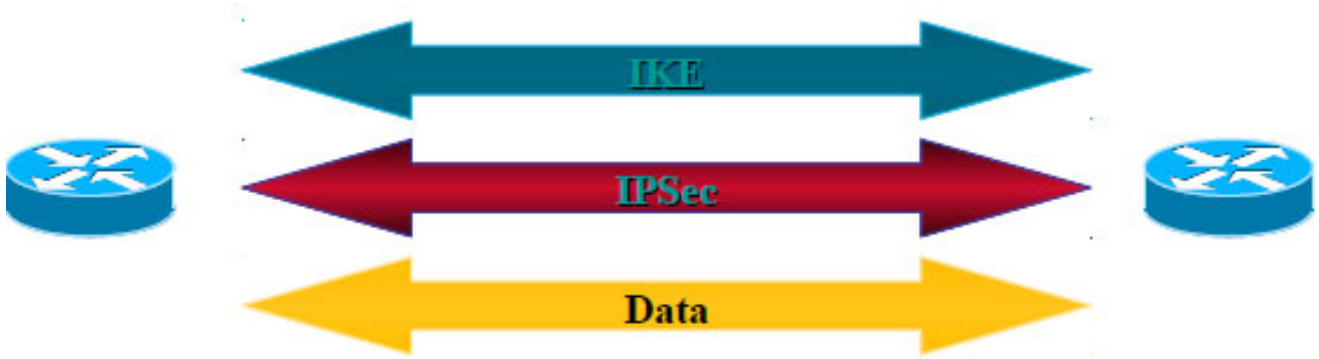


Inbound packet processing cont…



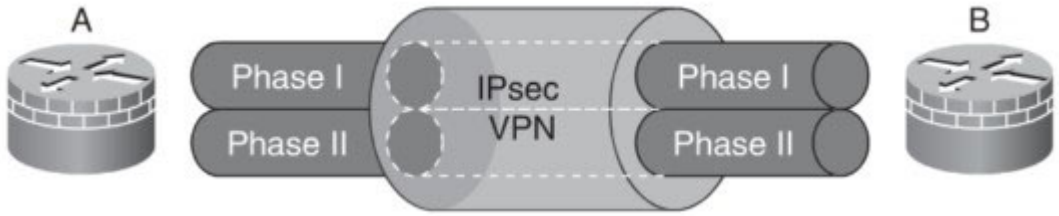
IKE

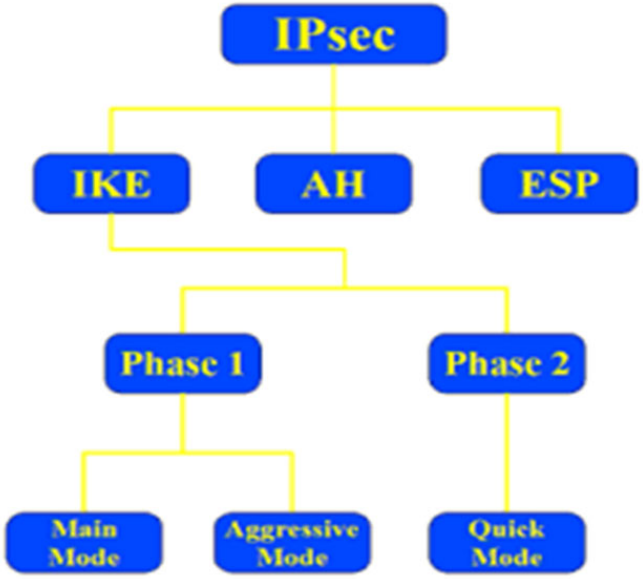
- The negotiated parameters (SA) need to be exchanged over a secure channel.
- Thus, before we can protect any IP packet, the two IPsec peers needs to build the IPsec tunnel.
- To establish an IPsec tunnel, Internet Key Exchange (IKE) protocol is used.
- The aim of the IKE protocol is to establish SAs and the aim of the IPsec protocols is to make use of these SAs.



IKE cont…

- IKE operates in 2 phases:
  - IKE Phase1 tunnel/ISAKMP tunnel: negotiate IKE SAs and establish a secure IKE tunnel. This phase can be operated in two different modes:
    - Main mode
    - Aggressive mode
  - IKE Phase2 tunnel/IPsec tunnel/quick mode: negotiate IPsec SAs and establish a secure IPsec tunnel that will be used to protect the actual transfer of user data between the two intranets.

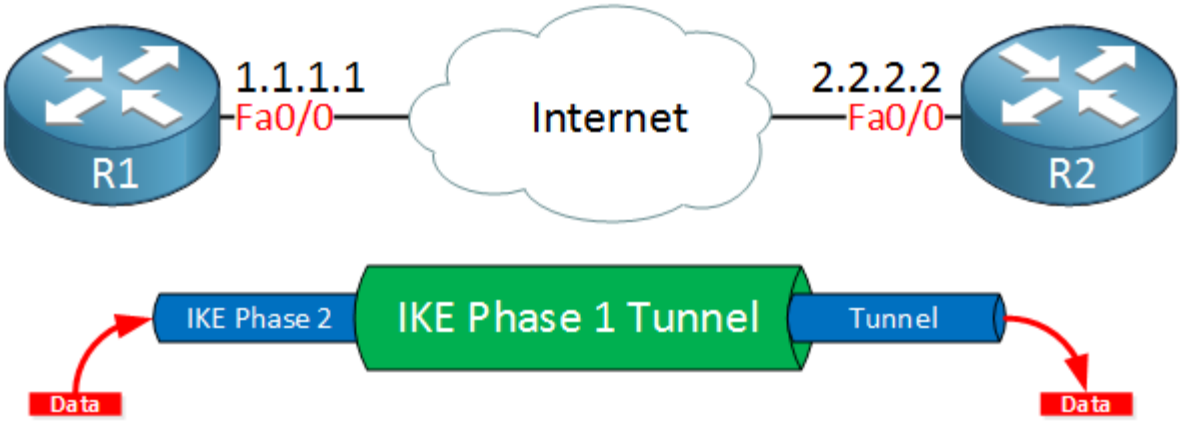




IKE cont…

- In IKE phase 1, two peers will negotiate about the encryption, authentication, hashing and other protocols that they want to use and some other parameters that are required. In this phase, an ISAKMP (Internet Security Association and Key Management Protocol) session is established. This is also called the ISAKMP tunnel/ IKE phase 1 tunnel.

- The IKE phase 1 tunnel is only used for management traffic. We use this tunnel as a secure method to establish the second tunnel called the IKE phase 2 tunnel/IPsec tunnel. Once IKE phase 2 is completed, we have an IKE phase 2 tunnel (or IPsec tunnel) that we can use to protect our user data. This user data will be sent through the IKE phase 2 tunnel.



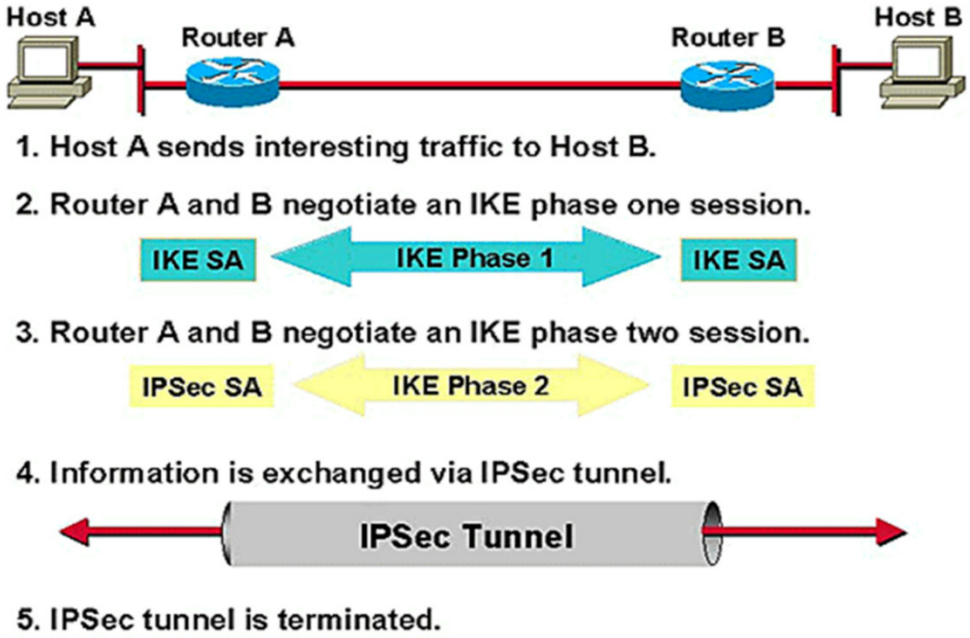
IKE cont…

- IKE builds the tunnels for us but it doesn't authenticate or encrypt user data. We use two other protocols for this:
  - AH (Authentication Header)
  - ESP (Encapsulating Security Payload)

- AH and ESP both offer authentication and integrity but only ESP supports encryption. Because of this, ESP is the most popular choice nowadays. Both protocols support two different modes:
  - Transport mode
  - Tunnel mode

Five Steps of IPsec

- Step1: Interesting Traffic: the traffic that should be protected (e.g. traffic that is permitted by the ACL).
- Step2: IKE Phase 1: IKE authenticates IPSec peers and negotiates IKE SAs during this phase, setting up a secure channel for negotiating IPSec SAs in phase 2.
- Step3: IKE Phase 2: IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers
- Step4: Data transfer: Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.
- Step5: Tunnel terminated: the tunnel is torn down. IPSec SAs terminate through deletion or by timing out.



IKEv1 and IKEv2

- The default setting is IKEv1 only.
- IKEv2 is automatically always used for IPv6 traffic.