IP security
Ipsec

La plupart des slides sont celles de Ahmed Serrouchni

Plan

- Présentation
- Services
- Architecture
- Protocole AH
- Protocole ESP
- L’association de sécurité
- Les politiques de sécurité
- Protocole IKE
- Conclusions

Présentation: motivations de IPSec

- IPSec (IP Security) est intégré dans IPv6
- Motivations de IPv6
  - Le protocole est définie pour répondre aux besoins de la future génération de l'Internet
  - Caractéristiques
    - Grande capacité d'adressage (128 bytes) avec un apport important pour alléger les tables de routage
    - Sécurisation des communications (IPSec)
    - Capacité de mise en œuvre de la qualité de service QoS
    - Protocole et architecture pour la mobilité
- 6bone un réseau mondial d'expérimentation de IPv6
- Stratégie de migration sont en cours de développement

Présentation: standardisation de IPSec

- IPSec = IP security Protocol
  - Standard développé à l'IETF
  - Premier RFC en 1995 sans gestion de clés
  - Deuxième version en Novembre 1998 avec la gestion des clés (IKE)
  - Partie commune entre IPv4 et IPv6 (obligatoire en IPv6)
- Implémentation de IPSec
  - Implémentation Native (dans la pile IP avec IPSec en native)
  - BITS (Bump in the Stack) : logiciel additionnel
  - BITW (Bump in the Wire) : processeur cryptographique externe

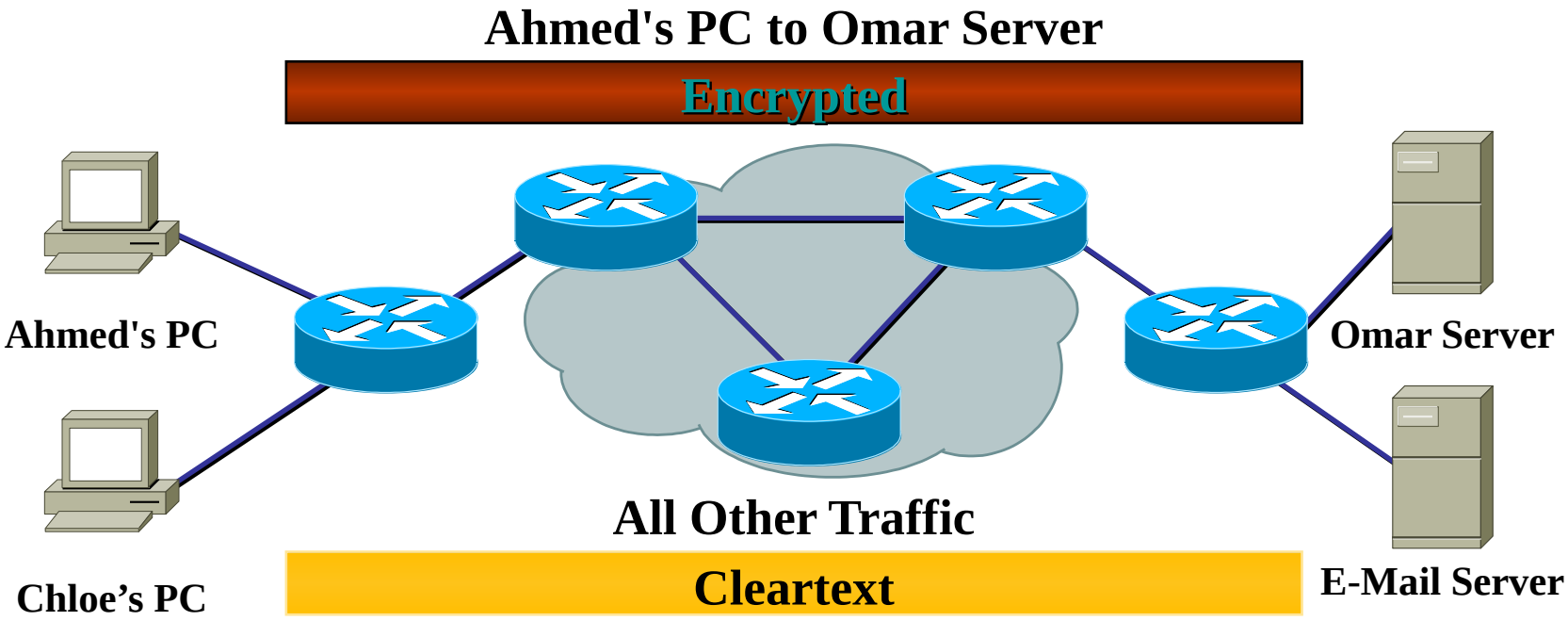
Présentation: bénéfice de IPSec

- IPSec
  - **Couche réseau pour le chiffrement et l'authentification**
  - Standards ouvert pour offrir des communications privés et sécurisés
  - Solution flexible pour déployer des politiques de sécurité à grande échelle
- Status de IPSec
  - Plusieurs RFCs bien définis
  - Plusieurs implémentations (Nortel, Redcreek, Sun Solaris, Microsoft, DEC, Cisco, HP, Telebit, 6Wind, Freeswan, etc.)
  - Plusieurs tests de conformance et d'interopérabilité basés sur des implantations de référence
- Caractéristiques de IPSec
  - Standard pour la confidentialité, l'intégrité, et l'authentification pour les échanges sur le réseau Internet
  - Transparent aux infrastructures du réseau
  - Solution de sécurité de bout en bout incluant routeurs, firewalls, PCs et serveurs

Services de sécurité fournis par IPsec

- Confidentialité des données
- Integrité des données
- Authentification de l’origine des données
- Contrôle d’accès
- Non rejeu

Architecture



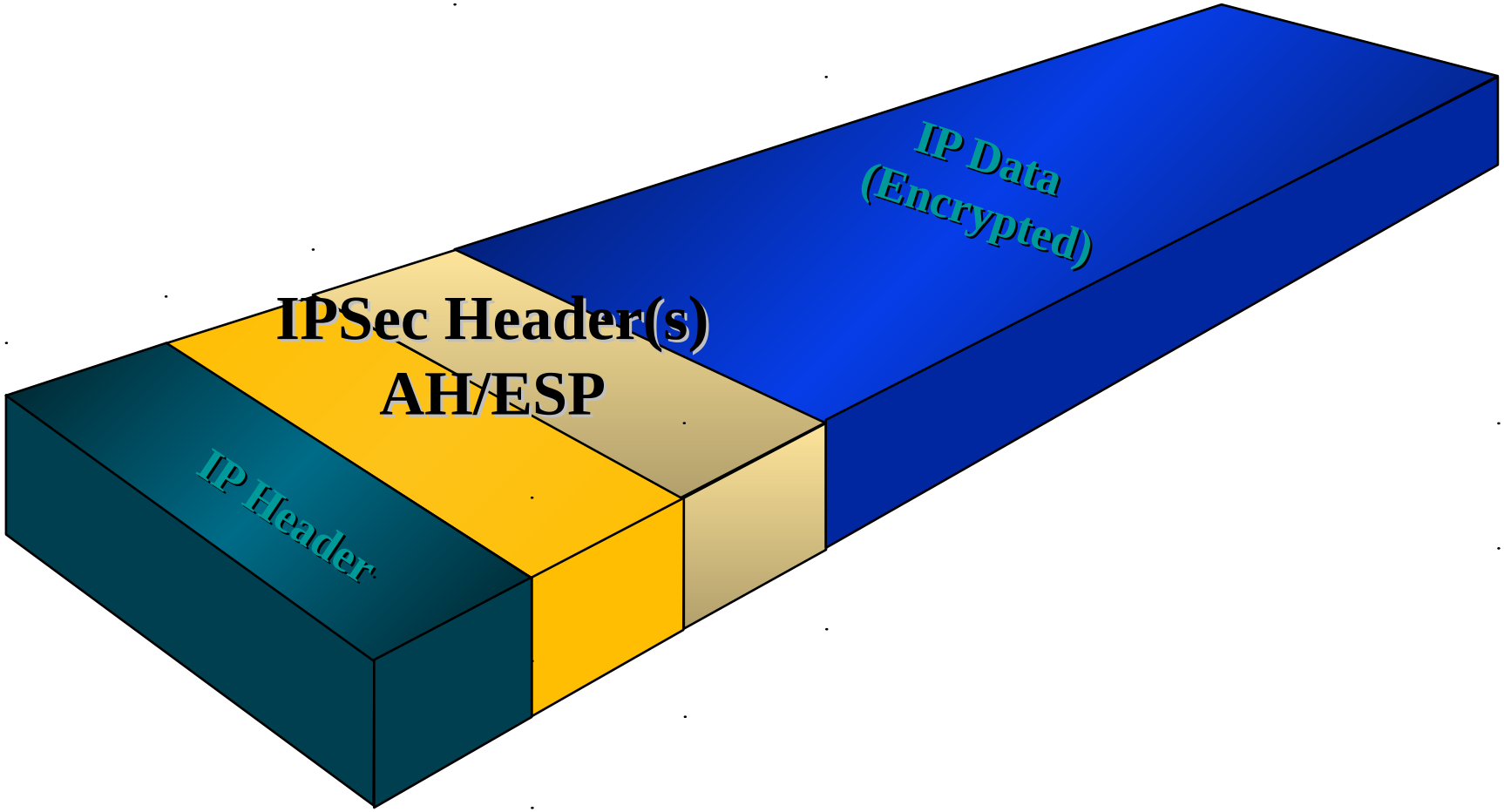
- Traffic protected on a flow-by-flow basis between specific hosts or subnets
- Media and interface independent
- Transparent to intermediate network devices
- Topology independent

Protocoles

- AH: Authentication Header
- ESP: EncapSuled Payload
- IKE: Internet Key Exchange
- ISAKMP
- OAKLEY

Protocole: encapsulation

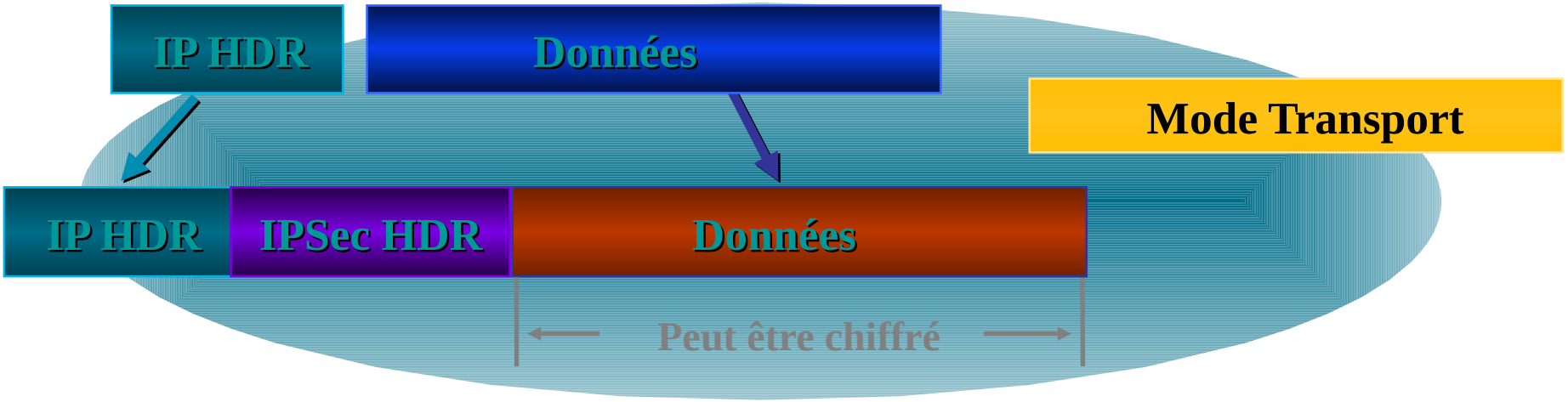
Interoperable Authentication, Integrity and Encryption



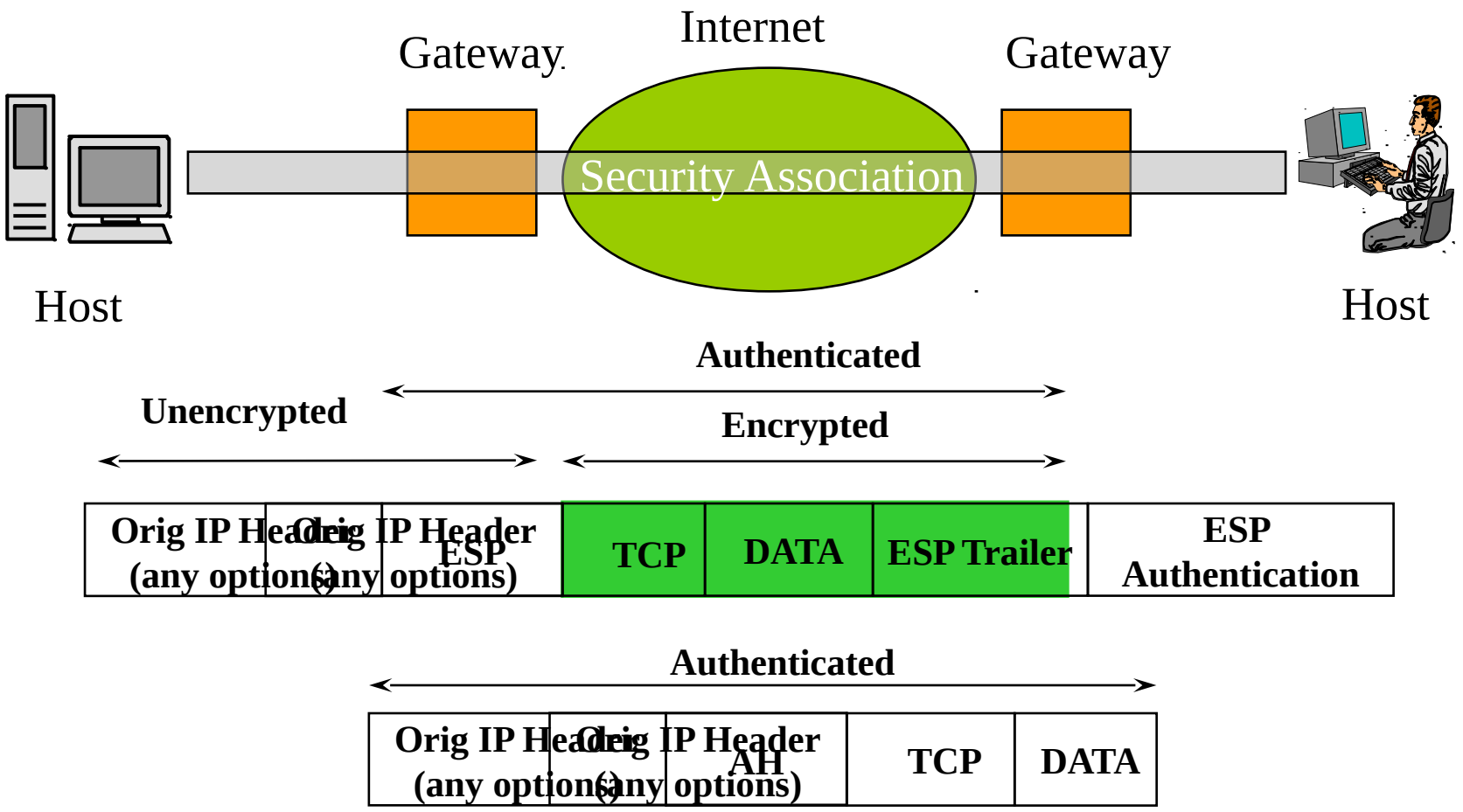
Protocole: mode Transport

- Dans le cas de la confidentialité seulement les données sont chiffrées
- Implémenter au dessus de IP

  - Special processing (like QoS, Multicast) enabled
  - Useful for tunneling protocol (like L2TP)

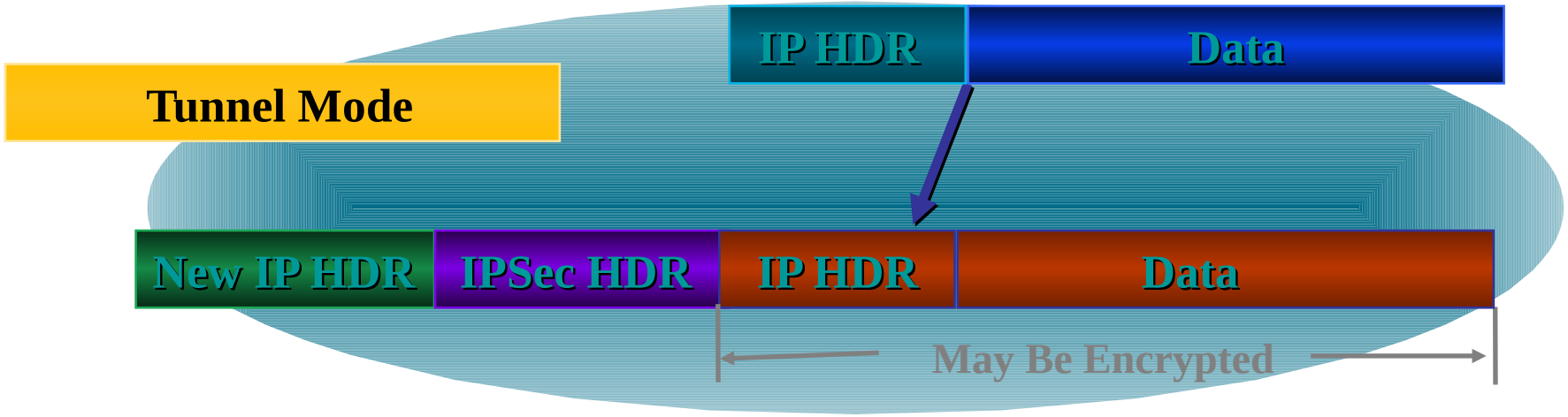


Architecture: IPSec Transport Mode

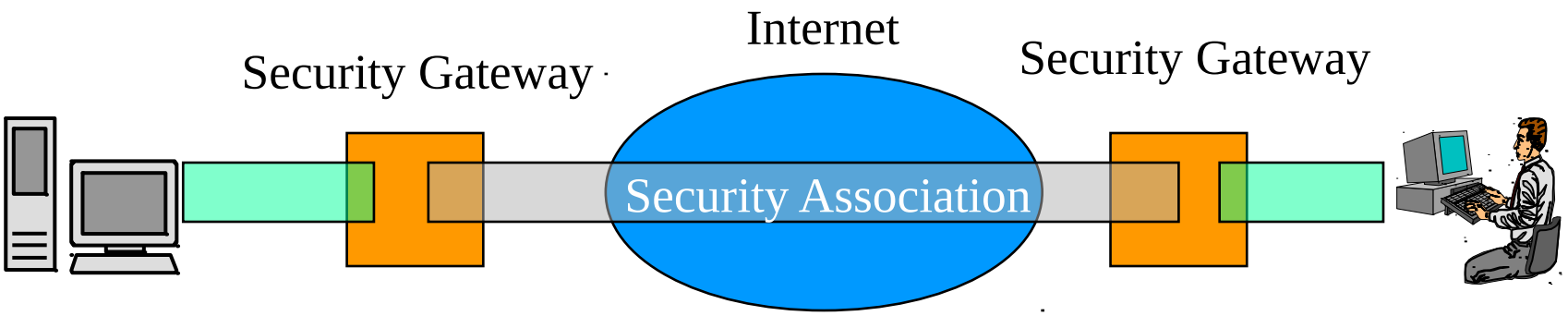


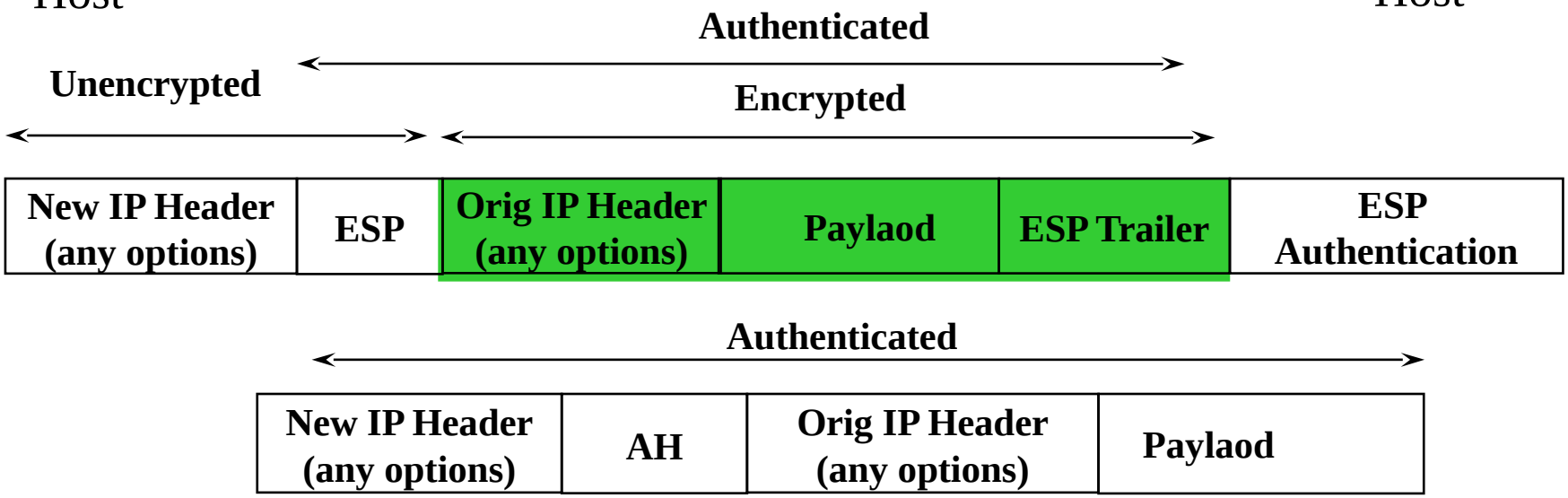
IPSec Tunnel Mode

- Tunnel mode
  - All IP datagram are encrypted
  - Implementation above IP
  - ESP tunnel mode :
    - can provide more security
    - less complexity and cost
  - Ideal for VPN



Architecture: IPSec Tunnel Mode



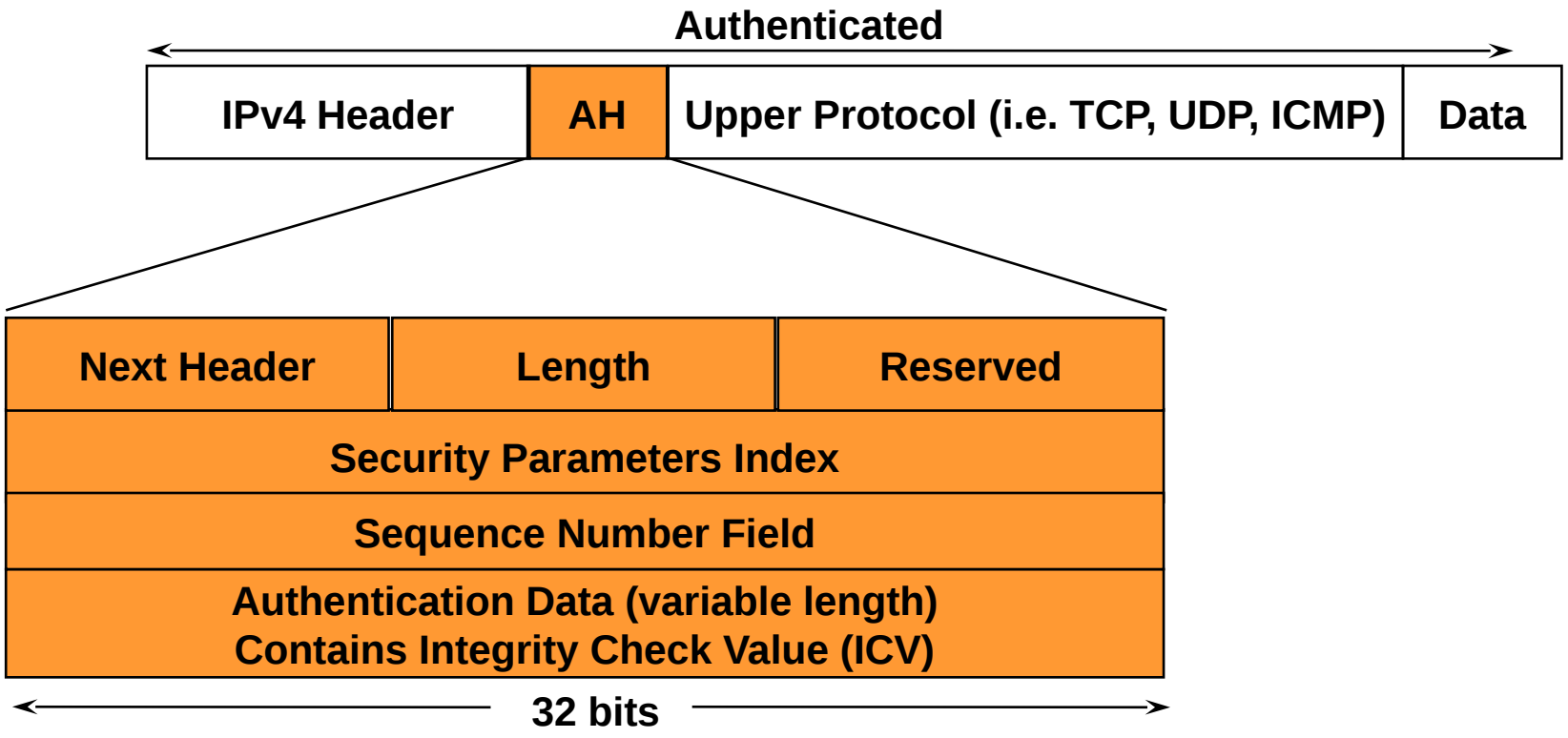


Authentication Header (AH)

- Data integrity
- Data origin authentication
- Anti-replay protection
- Protects the IP header
- No confidentiality

Protocol AH (Authentication Header)

- **Provides:**
  - Origin Authentication, Integrity, Anti-replay protection, does not provide encryption

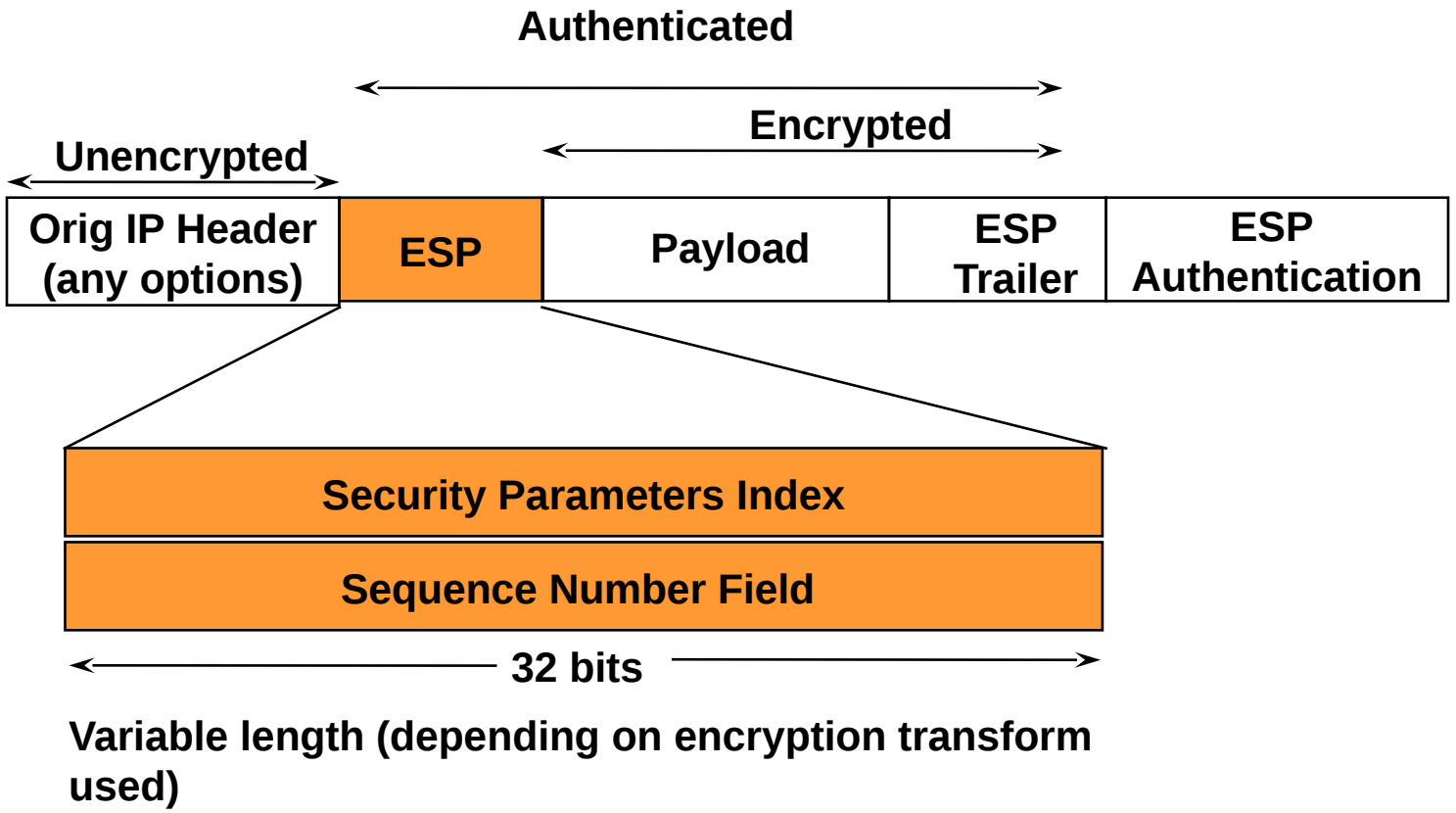


Protocol ESP: (Encapsulating Security Payload)

- Data confidentiality
- Limited traffic flow confidentiality
- Data integrity
- Data origin authentication
- Anti-replay protection
- Does not protect IP Header

Protocol ESP (Encapsulating Security Payload)

- Provides:
  - Confidentiality (Encryption), Origin Authentication, Integrity, Anti-replay protection

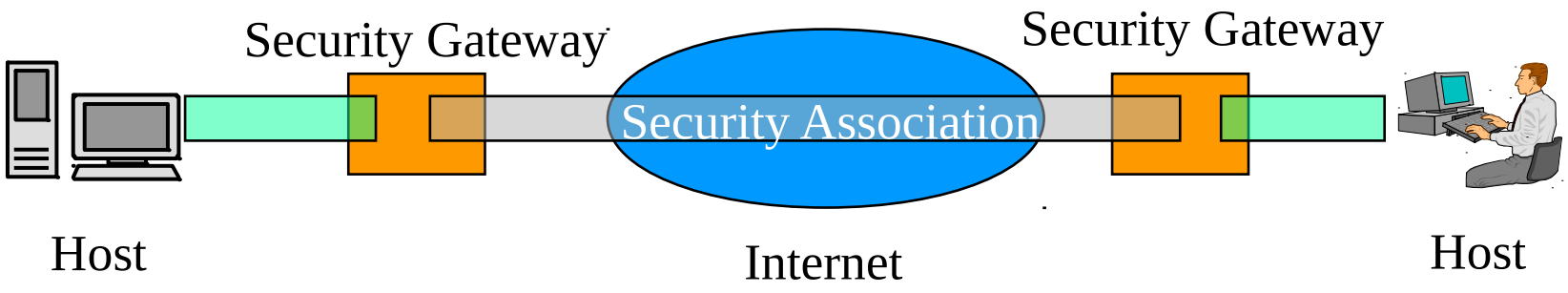


Security Association (SA)

- Defines a secure and unidirectional relationship
- Data structure containing the security parameters :
  - SPI (Security Parameter Index)
  - SNF (Sequence Number Field) used to avoid anti-replay
  - Anti-replay sequence number receive window
  - Authentication parameters (algorithms, keys, initialization vector)
  - Encryption parameters (algorithms, keys, length, initialization vector)
  - Key lifetime
  - SA lifetime
  - Protocol mode
  - PMTU
- For a typical bi-directional communication, two SAs (one in each direction) are needed)

Mechanisms: IPSec Security Associations

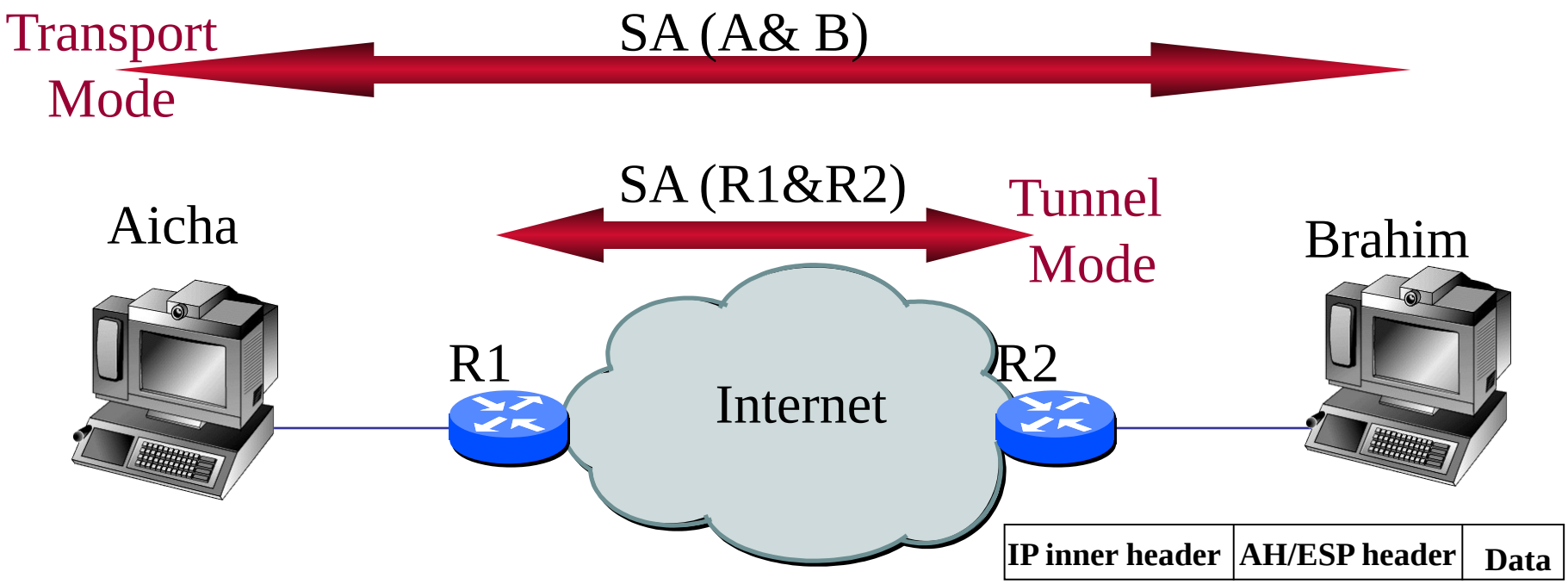
- A relationship between two or more entities that describes how the entities will use security services to communicate securely
- Simplex "connection" that affords security services to the traffic carried by it
- Bi-directional traffic requires one SA in each direction
- Security services provided by either AH or ESP
- If both AH and ESP required two SAs are formed
- Uniquely identified by
  - a SPI (Security Parameter Index)
  - IP destination address
  - Security Protocol Identifier (AH or ESP)



Security Association (SA)

- Agreement between two entities on a security policy, including:
  - Encryption algorithm
  - Authentication algorithm
  - Shared session keys
  - SA lifetime
- Unidirectional
  - Two-way communication consists of two Sas
- Key management
  - Manual mode
  - Automatic mode (via IKE)

Combining Security Associations



IP inner header	AH/ESP header	Data

IP outer header	AH/ESP header	IP inner header	AH/ESP header	Data

IP inner header	AH/ESP header	Data

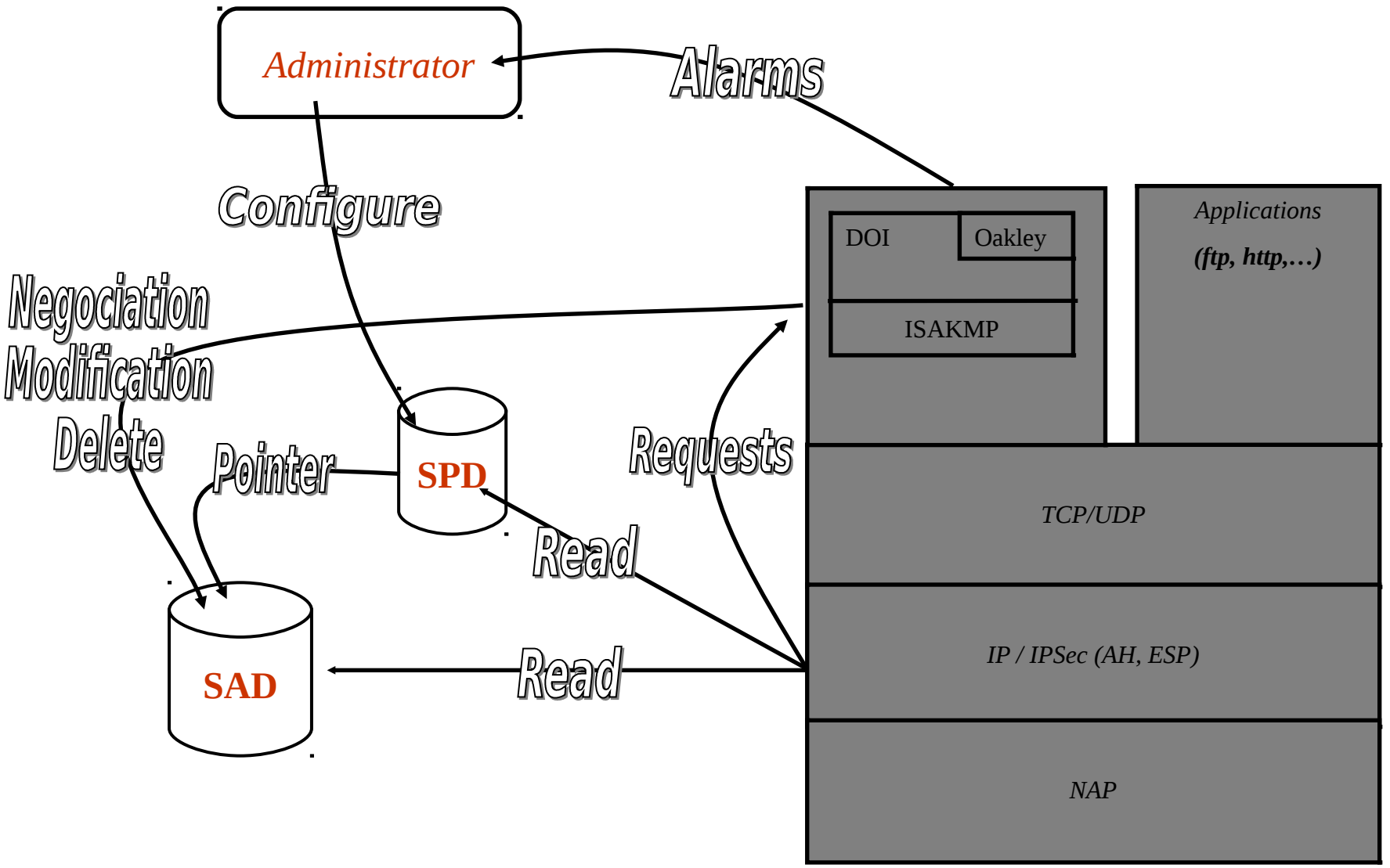
Security Policy Database (SPD)

- The SPD is the recipient for the system administrator’s specification, of the security policies to be applied to outbound and inbound traffic
- The nominal form of the SPD includes for each entry :
  - The selectors that defines the traffic to which the policy should be applied
  - The security policy to be applied to the packet matching the associated selectors
- Per interface, inbound and outbound SPDs

Security Association Database (SAD)

- The SAD contains the list of all inbound and outbound established SAs
- Each entry in the SAD defines the parameters associated with one SA. The entry is characterized by a set of values given to the field selectors. This defines the traffic flows to which the SA should be applied.
- For outbound processing, SAD entries are pointed to by entries in the SPD
- For inbound processing, each SAD entry is indexed by :
  - Outer header's destination IP address
  - IPSec protocol (AH or ESP) in the IP header (Protocol or Next Header fields)
  - SPI (Security Parameters Index) in the AH/ESP header : a 32-bit value used to distinguish among different SAs terminating at the same destination and using the same IPSec protocol

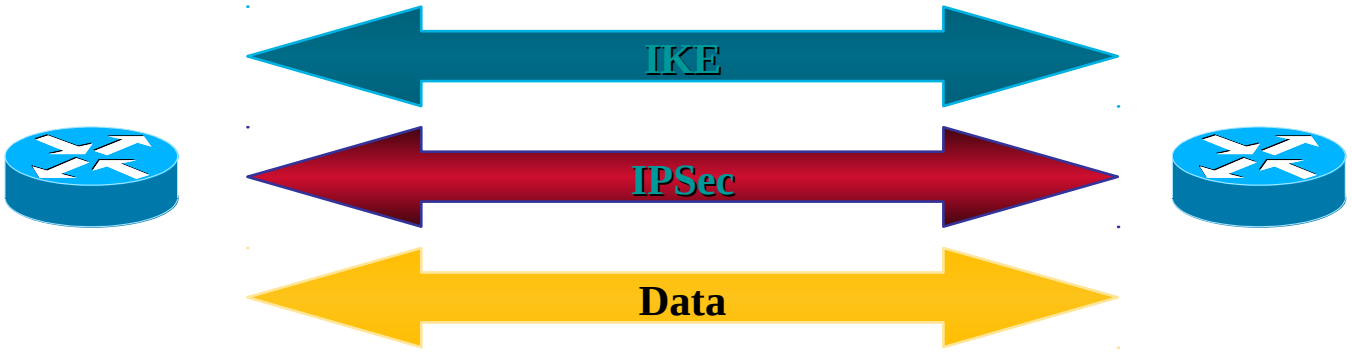
Mechanisms : Principle



Internet Key Exchange (IKE)

- IKE protocol
  - Negotiates policy to protect communication
  - Authenticated Diffie-Hellman key exchange
  - Negotiates (possibly multiple) security associations for IPSec
  - Hybrid of three earlier protocols
    - ISAKMP (payload, syntax and encoding)
    - OAKLEY (based on Diffie-Hellman)
  - Objective : offer a secure and automated IPSec SA negotiation
  - Two phase
    - Establishment of a secure channel between the two peers
      - Called ISAKMP Security Association
      - Negotiation of the ISAKMP parameters (Authentication method, Algorithms used for encryption and authentication)
      - Key exchange
    - Ipsec negotiation inside the ISAKMP secure channel
      - Negotiation of the IPSec parameters : security protocols, algorithms and keys used for data authentication and encryption

Initiating new connections

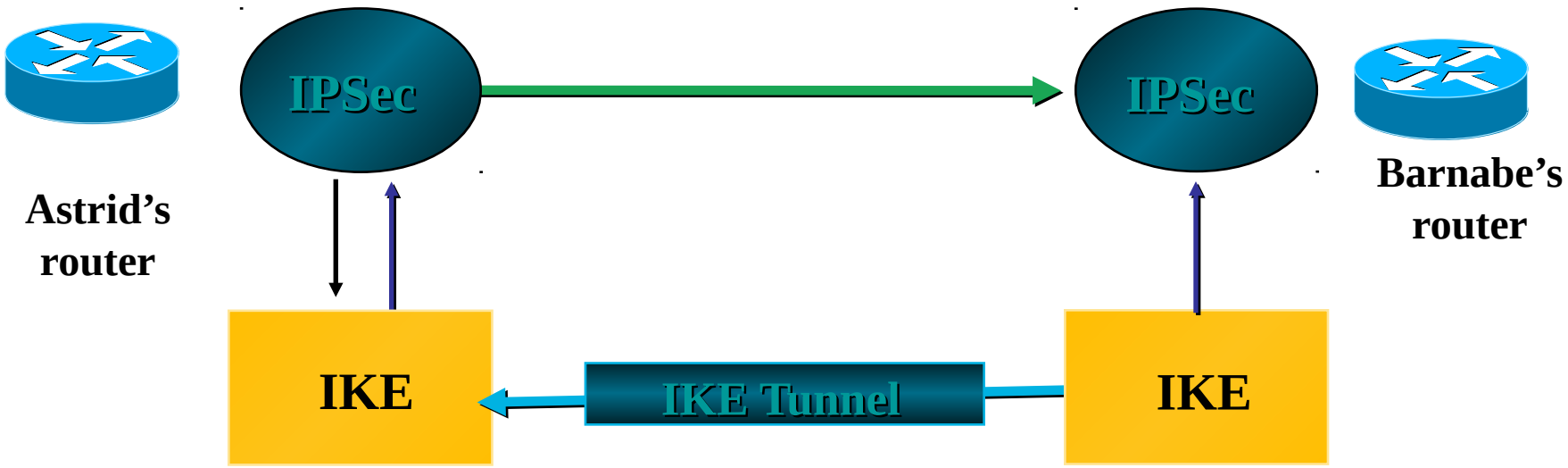


- **Establish IKE SA—“Main mode/Phase 1”**
- **Establish IPSec SA—“Quick mode/Phase 2”**
- **Send protected data**

How IPSec Uses IKE

1. Outbound packet from Astrid to Barnabe. No IPSec SA

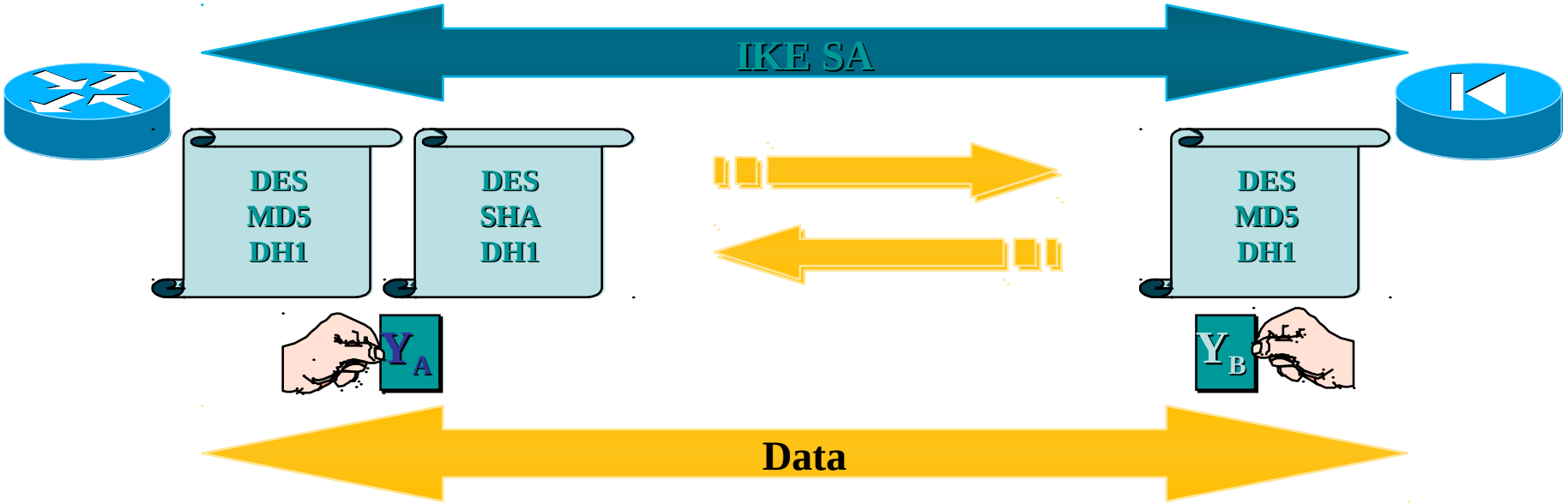
4. Packet is sent from Astrid to Barnabe protected by IPSec SA



2. Astrid's IKE begins negotiation with Barnabe's

3. Negotiation complete. Astrid and Barnabe now have complete set of SAs in place

Creating IPSec SA—Quick Mode



- **Requires IKE SA to be in place**
- **Negotiate IPSec parameters**
- **Create shared session key**

Local Policy

Exchange DH numbers for PFS or

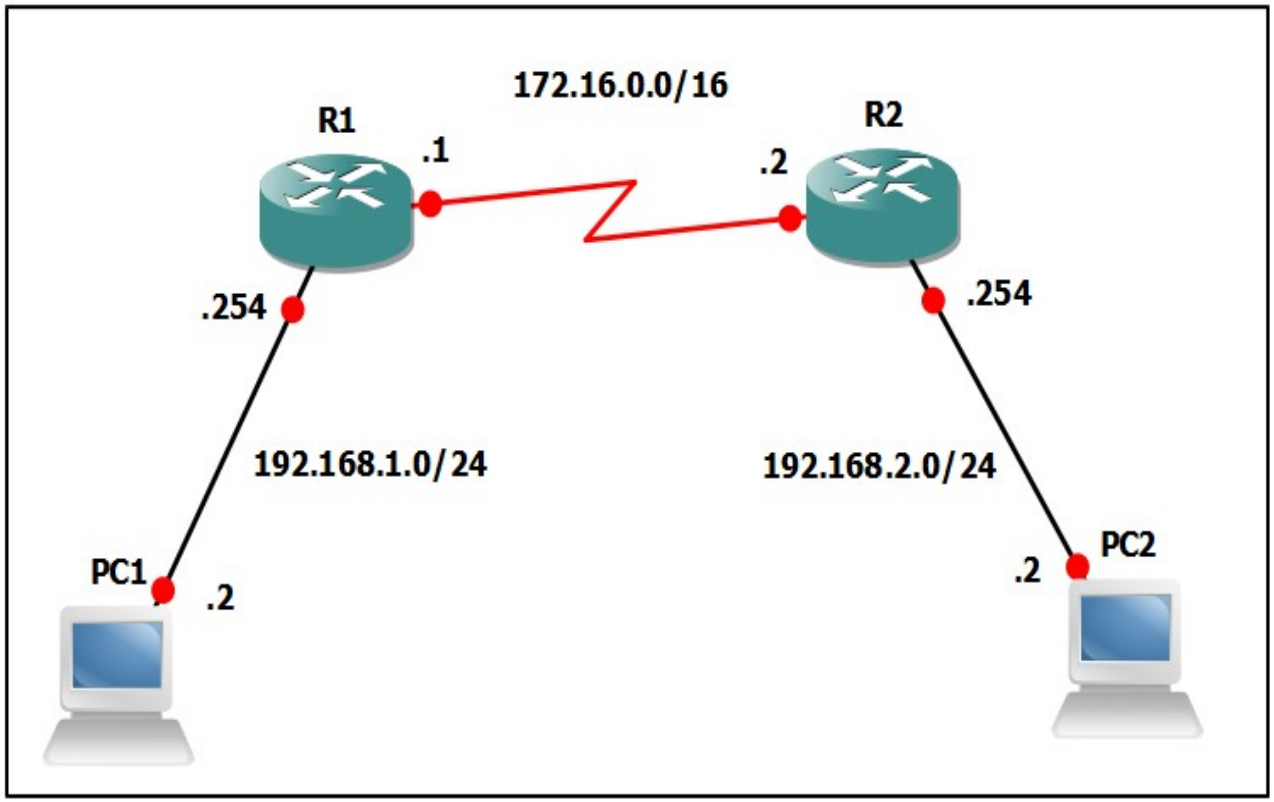
Exchange nonces for quick rekey

Conclusions

- IPSec is a whole system which can answer needs of security and could be adapted in a lot of situations
- The implementation of IPSec in IPv6 and his efficient adaptation in IPv4 assures IPSec to become one of the major security solutions of the Internet and Intranet in the future
- but some improvements have to be done …
  - Treatment packet by packet
  - Interoperability
    - NAT
    - Dynamic allocation address
    - Multicast
    - all IPSec implementations

Tunnels VPN-IPsec

- Exemple de tunnel VPN IPSec



Tunnels VPN-IPsec

- 5 étapes pour créer un tunnel VPN avec des routeurs cisco :
  - Configuration d'une politique ISAKMP
  - Configuration d'une clé pré-partagée pour ISAKMP
  - Configuration d'une transformation IPSec "transform-set"
  - Configuration d'une liste de contrôle d'accès pour le tunnel VPN
  - Apply the crypto map to the external interface.

```
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#encryption aes
R2(config-isakmp)#hash sha
R2(config-isakmp)#group 5
R2(config-isakmp)#exit
R2(config)#crypto isakmp key isi-master-ssice add 172.16.0.1
R2(config)#crypto ipsec transform-set esp-aes-sha esp-aes esp-
sha-hmac
R2(cfg-crypto-trans)#exit
R2(config)#$access-list 101 permit ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255
R2(config)#crypto map vpn 10 ipsec-isakmp
R2(config-crypto-map)#match add 101
R2(config-crypto-map)#set transform-set esp-aes-sha
R2(config-crypto-map)#set peer 172.16.0.1
R2(config-crypto-map)#exit
R2(config)#int s0/0
R2(config-if)#crypto map vpn
R2(config-if)#end
```

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption aes
R1(config-isakmp)#hash sha
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key isi-master-ssice add 172.16.0.2
R1(config)#crypto ipsec transform-set esp-aes-sha esp-aes esp-
sha-hmac
R1(cfg-crypto-trans)#exit
R1(config)#$ access-list 101 permit ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255
R1(config)#crypto map vpn 10 ipsec-isakmp
R1(config-crypto-map)#match add 101
R1(config-crypto-map)#set transform-set esp-aes-sha
R1(config-crypto-map)#set peer 172.16.0.2
R1(config-crypto-map)#exit
R1(config)#int s0/0
R1(config-if)#crypto map vpn
R1(config-if)#end
```