IP SECURITY (IPSec)

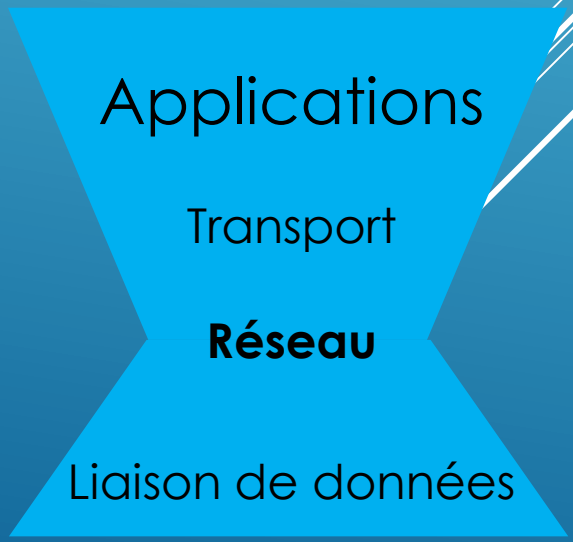
RFC 2401

INTRODUCTION

- Les VPNs peuvent s'appliquer n'import quelle couche du modèle OSI:
  - Apps: FTP, SMTP, MIME, SSH …
  - Transport: TCP, UDP
  - Réseau: IP
  - Liaison de données: Ethernet, Wi-Fi, 3G, 4G …

Exemple:

- TLS (SSL)+HTTP=HTTPs
- SSH : crypter et authentifier



IPSec

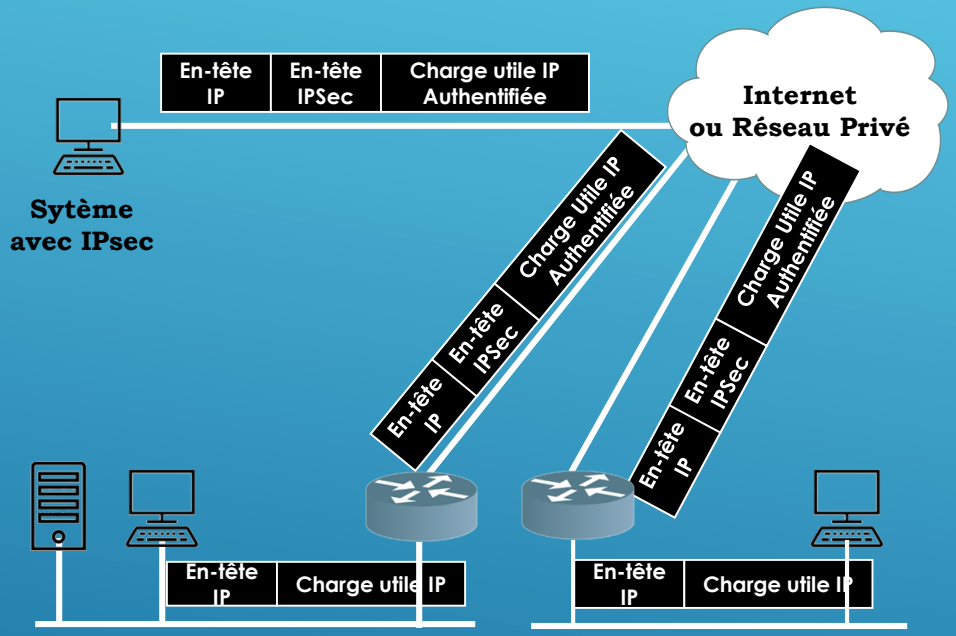
- Besoin d'une suite de protocoles qui serve de « **FrameWork** » pour négocier les paramètres entre deux nœuds IP distants.
- Les services de sécurité:
  - Confidentialité
  - Contrôle d'accès
  - Intégrité
  - Authentification
  - Protection contre le rejeu (anti-replay protection), « séquencement »

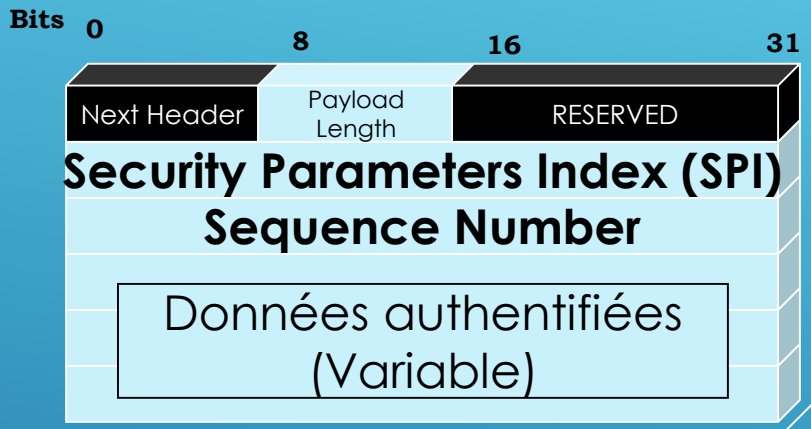
IPSec | PROTOCOLES ET ÉLÉMENTS CLÉS

- Protocoles de sécurité:
  - Authenticaton Header (AH)
  - Encapsulation Payload (ESP)
- Protocole de négociation
  - Internet Key Exchange (IKE)
  - Internet Security Association Key Management Protocol (ISAKMP)
  - Security Association (SA)
- Cryptage: DES, 3DES, AES
- Authentification: H-MAC (MD5, SHA)
- Protection (Clés de session) : DH1, DH2, DH5, DH7

MODÈLE AH

Routeur avec IPSec



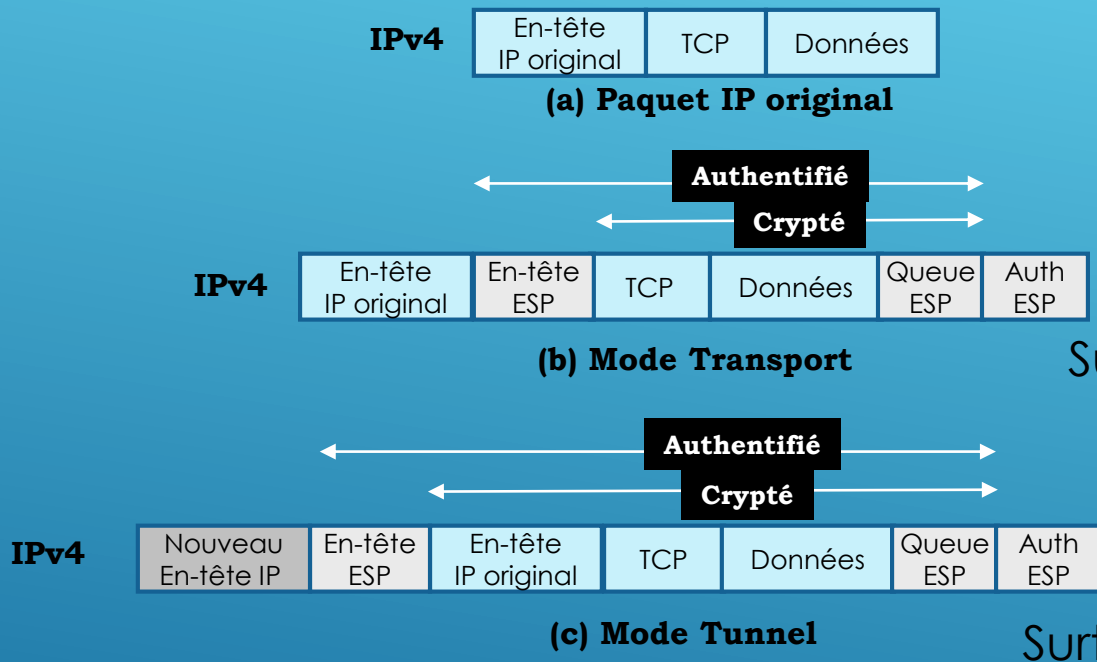


Index du paramètre de sécurité (SPI)
identifie les paramètres de sécurité

Numéro de séquence
un compteur qui évite les attaques par répétitio

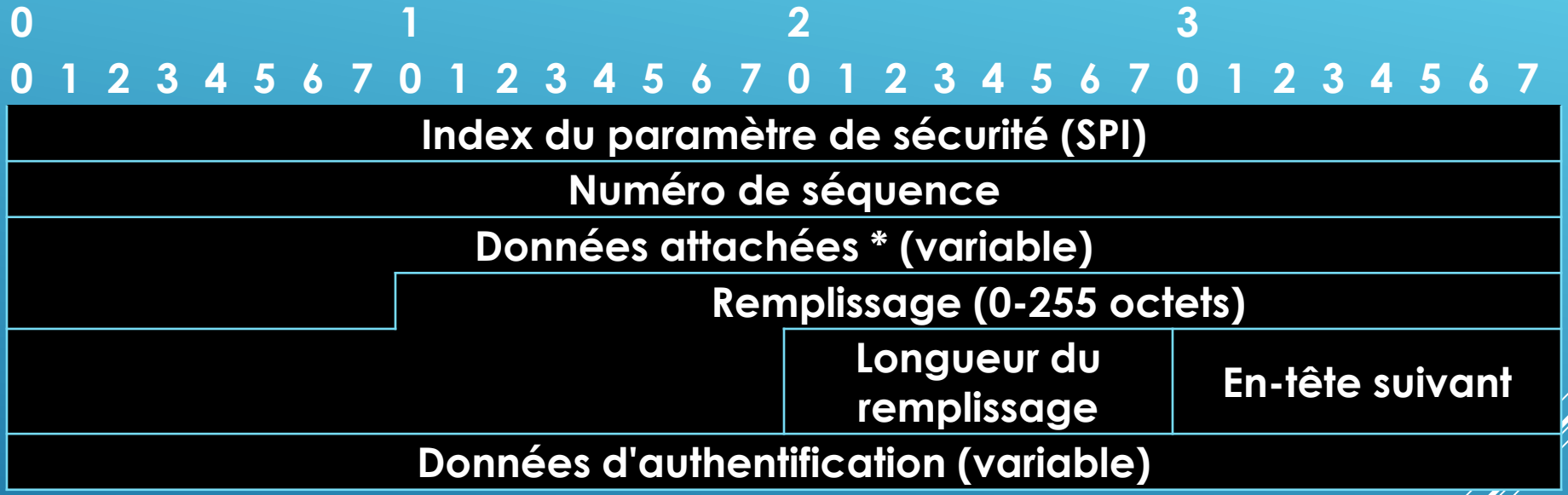
- **AH (Authentication Header) - Protocole de sécurité qui fournit l'authentification, l'intégrité des données et un service optionnel de détection d'intrusion. AH est dans la charge utile du paquet.**

MODÈLE ESP



- **ESP (Encapsulation Security payload) - Protocole de sécurité qui fournit la confidentialité, l'intégrité des données et des services de protection, des services optionnels d'authentification de l'origine des données et de détection d'intrusion. ESP encapsule les données à protéger.**

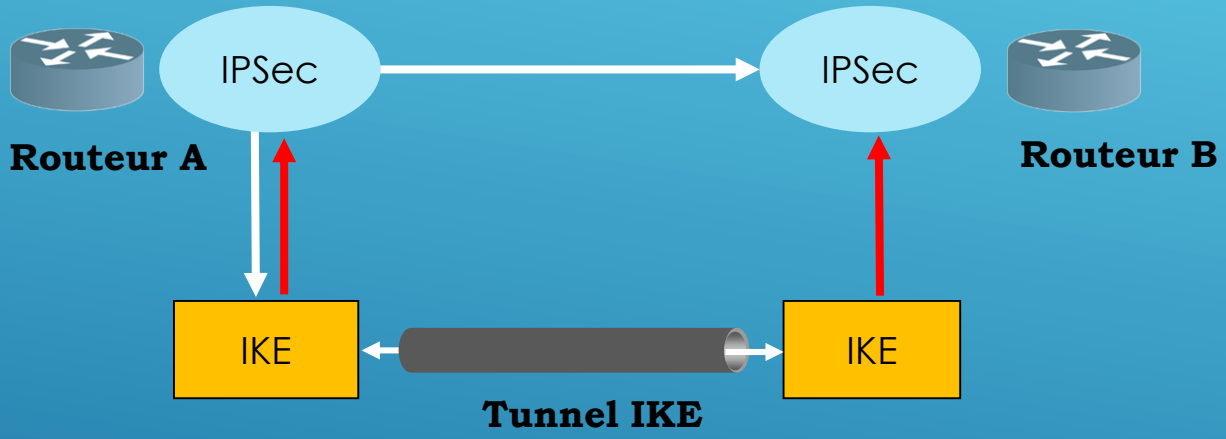
EN-TETE ESP



Index du paramètre de sécurité (SPI)
identifie les paramètres de sécurité

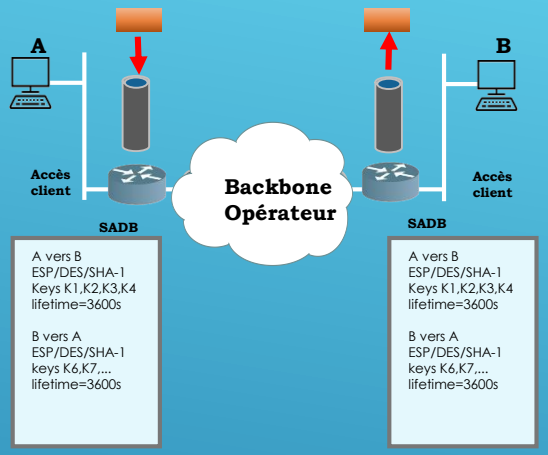
Numéro de séquence
un compteur qui évite les attaques par répétition

IKE « INTERNET KEY EXCHANGE »



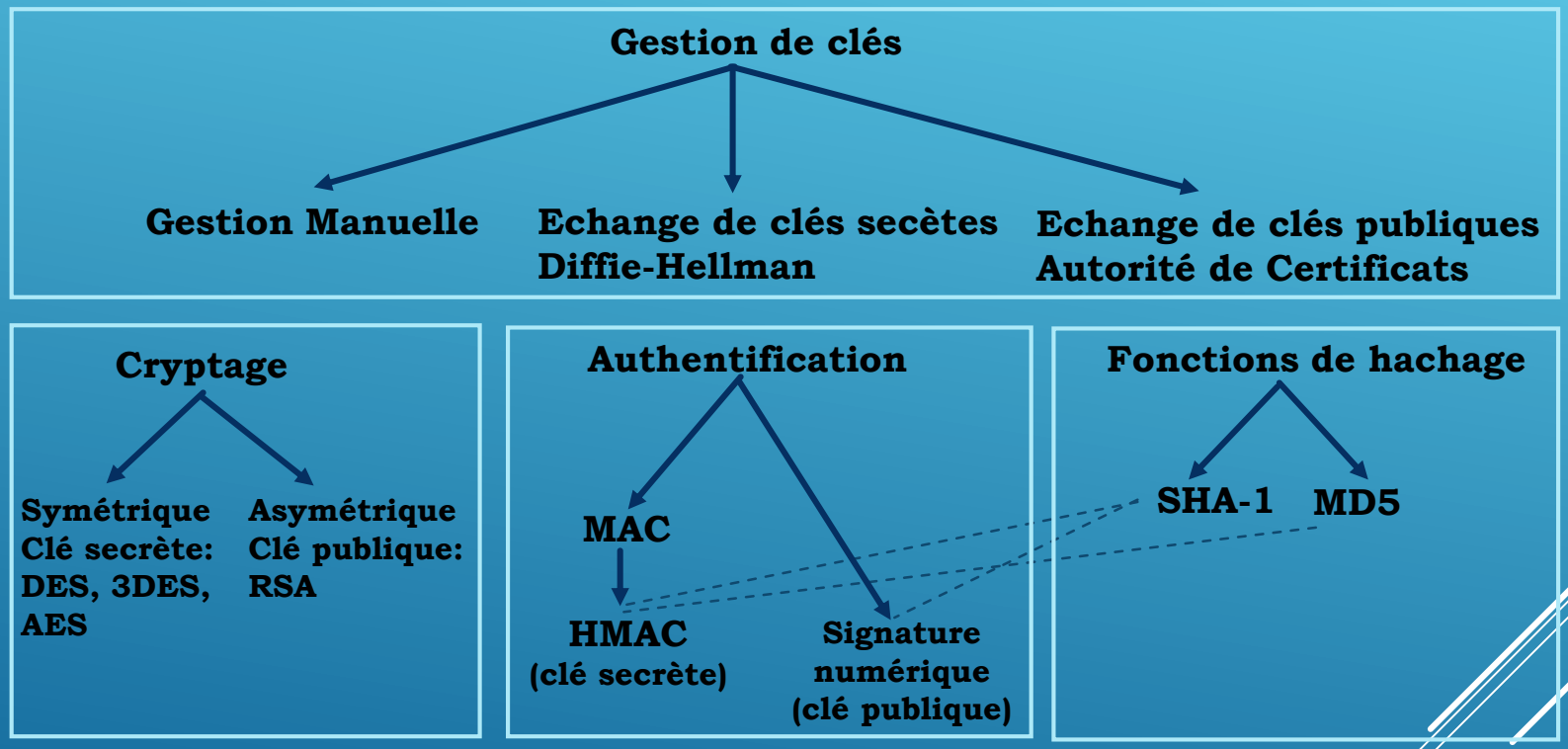
- **IKE : Protocole hybride qui implémente l'échange de clés Oakley et l'échange de clés Skeme dans le cadre de ISAKMP. Oakley et Skeme définissent chacun une méthode pour établir un échange de clés authentifié. Ceci inclut la construction de la charge utile, les informations transportées dans la charge utile, l'ordre dans lequel les clés sont traitées et comment elles sont utilisées.**

ISAKMP | SA



- **SA (Security Association) : Ensemble de principes (politiques) et de clés utilisés pour protéger l'information. La SA ISAKMP est la politique commune et les clés utilisées par les extrémités qui négocient dans ce protocole pour protéger leur communication.**
- **ISAKMP : (Internet Security Association and Key Management Protocol) : Un protocole cadre qui définit le format des charge utiles, les mécanismes d'implémentation d'un protocole d'échange de clés et la négociation d'une SA.**

SYSTÈME DE CRYPTAGE



PRÉSENTATION IPSEC

- **Le RFC 2401 décrit la trame générale de l'architecture IPSec**
- **Comme tous les mécanismes de sécurité, le RFC 2401 aide à la mise en œuvre d'une politique de sécurité.**
- **La politique de sécurité définit les besoins de sécurité pour différentes connexions.**
- **Les connexions sont des sessions IP**
- **La trame générale de l'architecture IPSec fournit:**
  - **Intégrité des données**
  - **Authentification**
  - **Confidentialité des données**
  - **Associations de sécurité**
  - **Gestion des clés**

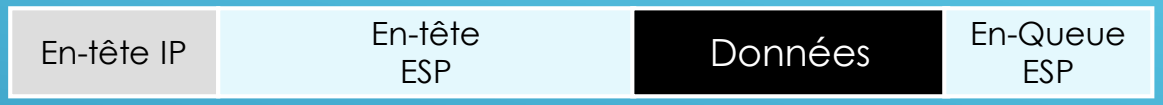
IPSEC | AUTHENTICATION HEADER (AH)

- **L'Authentification Header (AH) IP est utilisé pour fournir l'intégrité, l'authentification de l'origine des données pour des paquets IP et fournit également la détection de l'intrusion d'un tiers dans l'échange.**
- **Le service de détection d'intrusion d'un tiers dans l'échange est optionnel. Si celui-ci est négocié et validé, il faut que le récepteur teste les numéros de séquence.**
- **AH fournit l'authentification pour l'en-tête IP et TCP mais certains champs de l'en-tête changent au cours du transit dans le réseau.**
- **AH ne peut pas fournir de protection complète de l'en-tête IP**

IPSEC | AUTHENTICATION HEADER (AH)

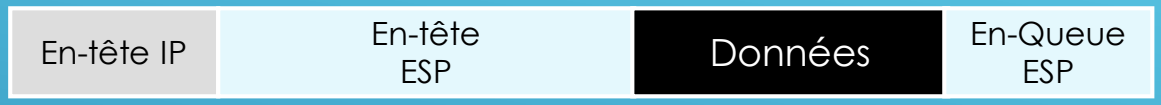
- **AH peut être appliqué seul, en combinaison avec IP ESP ou de manière imbriquer au travers de l'utilisation du mode tunnel.**
- Les services de sécurité peuvent être fournis entre une paire de hosts, une paire de passerelles de sécurité ou entre une passerelle de sécurité et un host.
- **ESP peut être utilisé pour fournir les mêmes services plus la confidentialité (cryptage).**
- La différence principale entre les services d'authentification de AH et ESP est l'extension de la couverture.
- ESP ne protège pas les champs de l'en-tête IP à moins que cet en-tête soit encapsulé par ESP (Mode tunnel).

IPSEC | ENCAPSULATION SECURITY PAYLOAD (ESP)



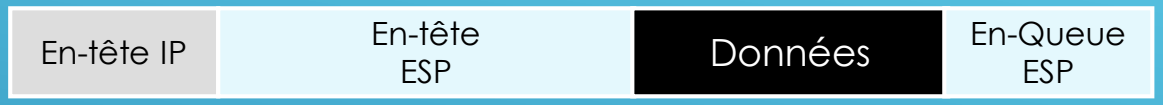
- **L'en-tête ESP est inséré après l'en-tête IP et avant l'en-tête de protocole de couche supérieure dans le mode transport ou avant un en-tête IP encapsulé en mode tunnel.**
  ESP est utilisé pour fournir les services suivants:
  - **Confidentialité**
  - **Authentification de l'origine des données**
  - **Intégrité**
  - **Service de détection d'intrusion d'une tierce partie dans l'échange**

IPSEC | ENCAPSULATION SECURITY PAYLOAD (ESP)



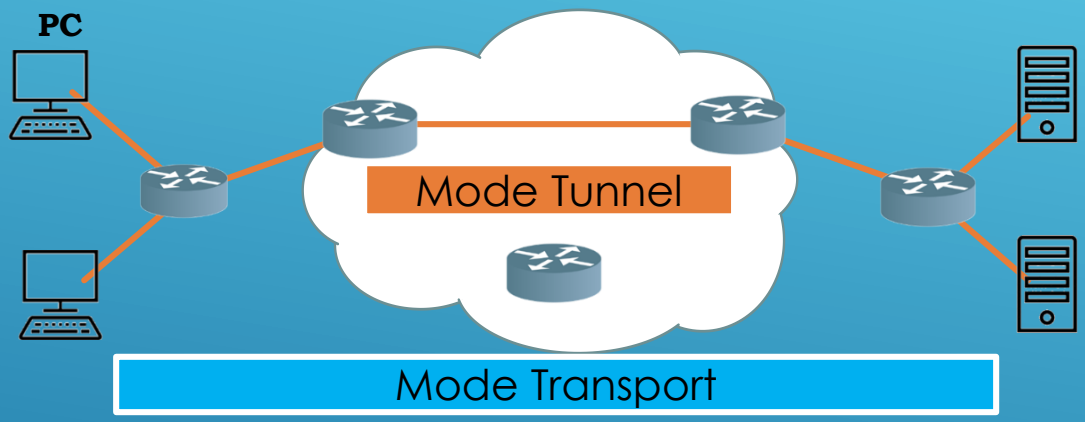
- **L'ensemble des services fournis dépend des options sélectionnées au moment de l'établissement des associations de sécurité et l'emplacement de l'implémentation.**
- **La confidentialité peut être sélectionnée indépendamment des autres services.**
- **Cependant l'utilisation de la confidentialité sans intégrité/authentification, soit dans ESP ou séparément dans AH peut rendre certains trafics vulnérables à des attaques actives.**

IPSEC | ENCAPSULATION SECURITY PAYLOAD (ESP)



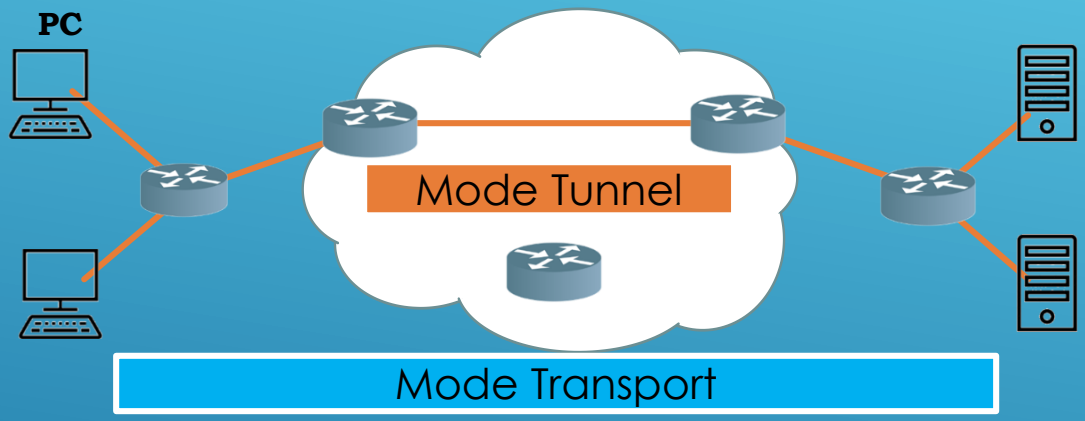
- **L'authentification de l'origine des données et l'intégrité sont des services joints et sont offerts en option conjointement avec la confidentialité optionnelle.**
- **Le service de détection d'intrusion d'une tierce partie peut être sélectionné que si l'authentification de l'origine des données est sélectionnée et reste entièrement à la discrétion du receveur.**
- **Le service de détection d'intrusion d'une tierce partie sera effectivement actif uniquement si le receveur teste les numéros de séquence.**
- **La confidentialité de trafic nécessite la sélection du mode tunnel.**
- **Bien que la confidentialité et l'authentification soient optionnelles au moins une des deux doit être sélectionnée.**

IPSEC | MODE TUNNEL CONTRE MODE TRANSPORT



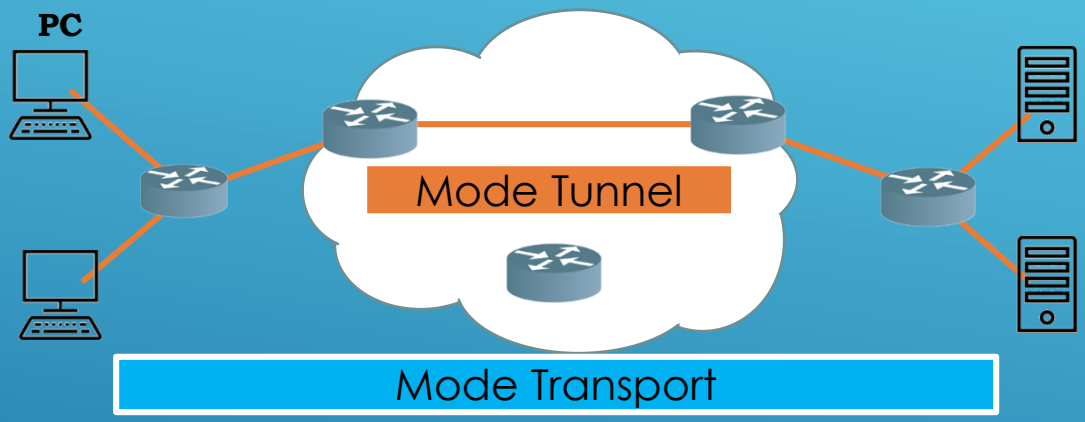
- **En mode Transport les hôtes d'extrémité réalisent l'encapsulation IPSec de leurs propres données (host à host) par conséquent IPSec doit être implémenté sur chacun des hosts.**
  - **L'application des points d'extrémité doit être aussi une extrémité IPSec.**
- **En mode Tunnel les passerelles IPSec fournissent les services IPSec aux autres hosts dans des tunnels point à point. Les hosts d'extrémité n'ont pas besoin d'avoir IPSec.**

IPSEC | MODE TUNNEL CONTRE MODE TRANSPORT



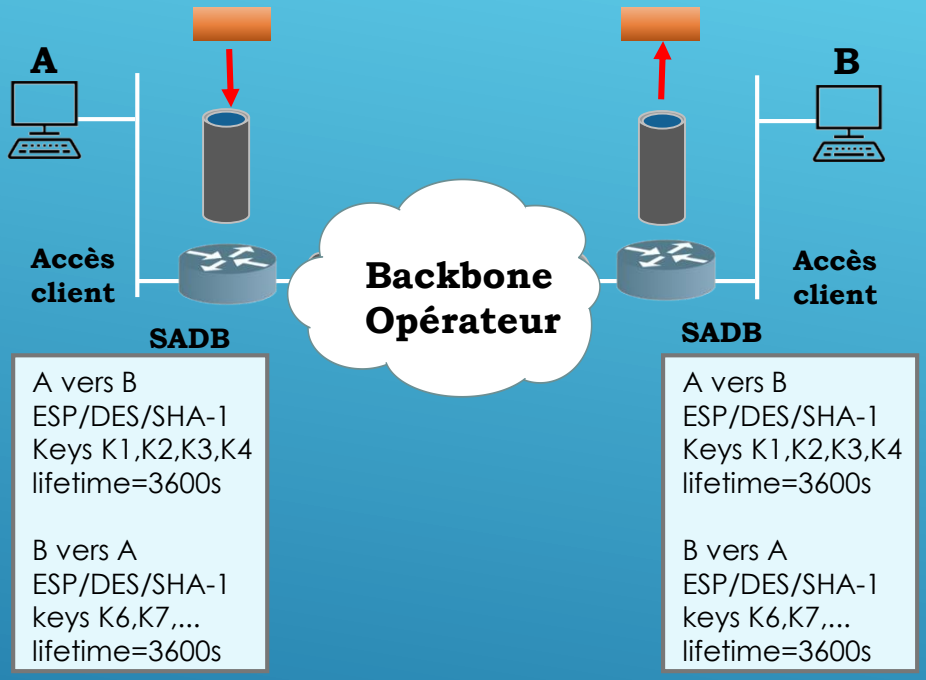
- **ESP peut être appliqué aux paquets IP de deux façons différentes:**
  - **Le mode Transport fournit la sécurité aux couches de protocoles supérieures.**
  - **Le mode Transport protège la charge utile du paquet mais garde l'adresse IP originale en clair.**
  - **L'adresse IP originale est utilisée pour router les paquets sur Internet.**
  - **Le mode Transport ESP est utilisé entre hosts.**

IPSEC | MODE TUNNEL CONTRE MODE TRANSPORT



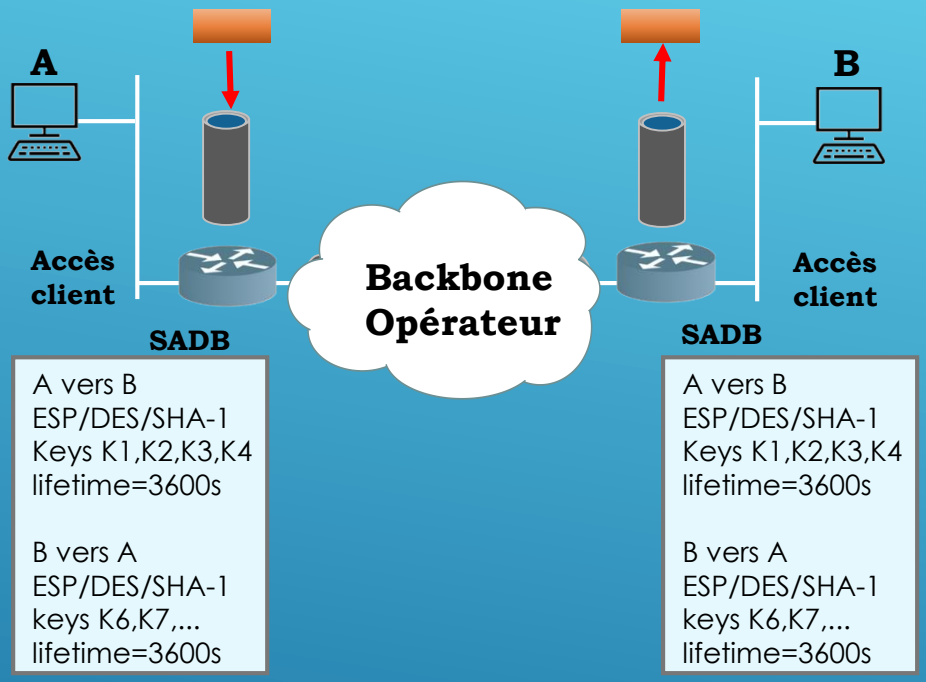
- **ESP peut être appliqué aux paquets IP de deux façons différentes:**
- **Le mode Tunnel fournit la sécurité pour tout le paquet IP.**
  - **Le paquet IP original est crypté**
  - **Le paquet crypté est encapsulé dans un autre paquet IP.**
  - **L'adresse IP "outside" est utilisée pour router les paquets sur Internet .**

IPSEC | SECURITY ASSOCIATION (SA)



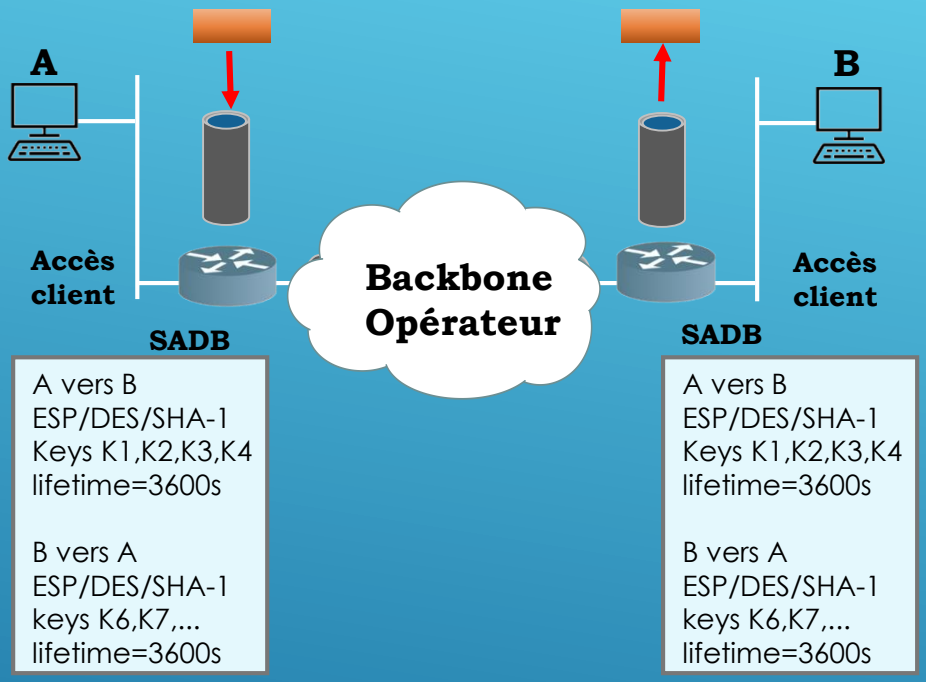
- **Les SAs ou Secutity Associations sont un concept de base très important dans IPSec**
- **Elles représentent un contrat entre deux extrémités et décrivent comment ces deux extrémités vont utiliser les services de sécurité IPSec pour protéger le trafic.**
- **Les SAs contiennent tous les paramètres de sécurité nécessaires pour sécuriser le transport des paquets entre les deux extrémités et définissent la politique de sécurité utilisée dans IPSec.**

IPSEC | SECURITY ASSOCIATION (SA)



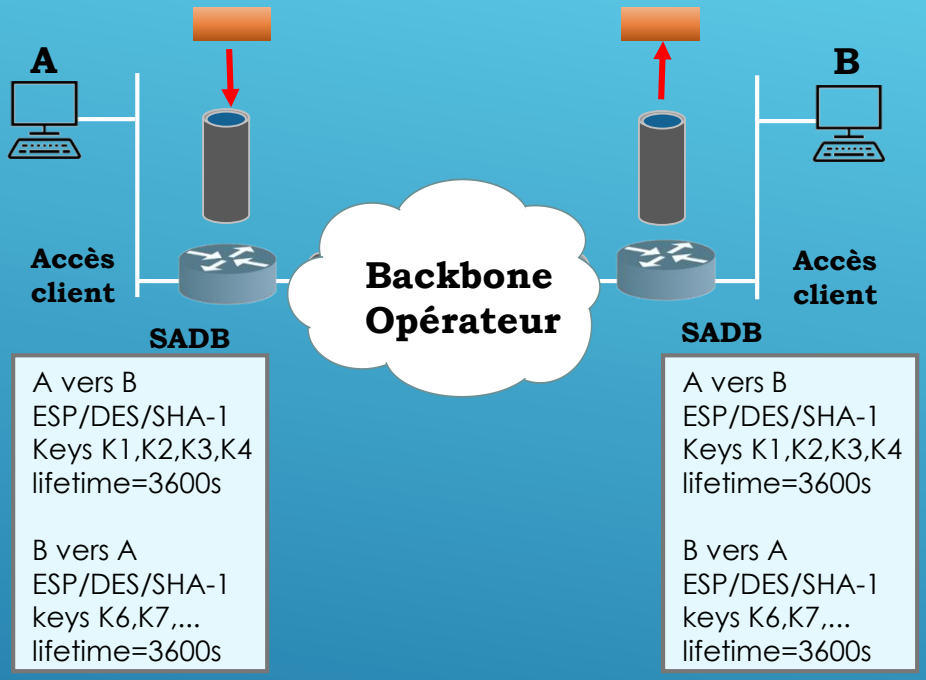
- **Les routeurs ont besoin de deux SAs pour protéger le trafic entre les hosts A et B.**
- **L'établissement des SAs est un prérequis dans IPSec pour la protection du trafic.**
- **Quand les SAs appropriées sont établies, IPSec se réfère à celles-ci pour obtenir tous les paramètres nécessaires à la protection du trafic**
- **Une SA doit mettre en vigueur la politique de protection en ces termes: Pour le trafic entre A et B, utilisez ESP 3DES avec les clés K1,K2 et K3 pour le cryptage de la charge utile, SHA-1 avec la clé K4 pour l'authentification.**

IPSEC | SECURITY ASSOCIATION (SA)



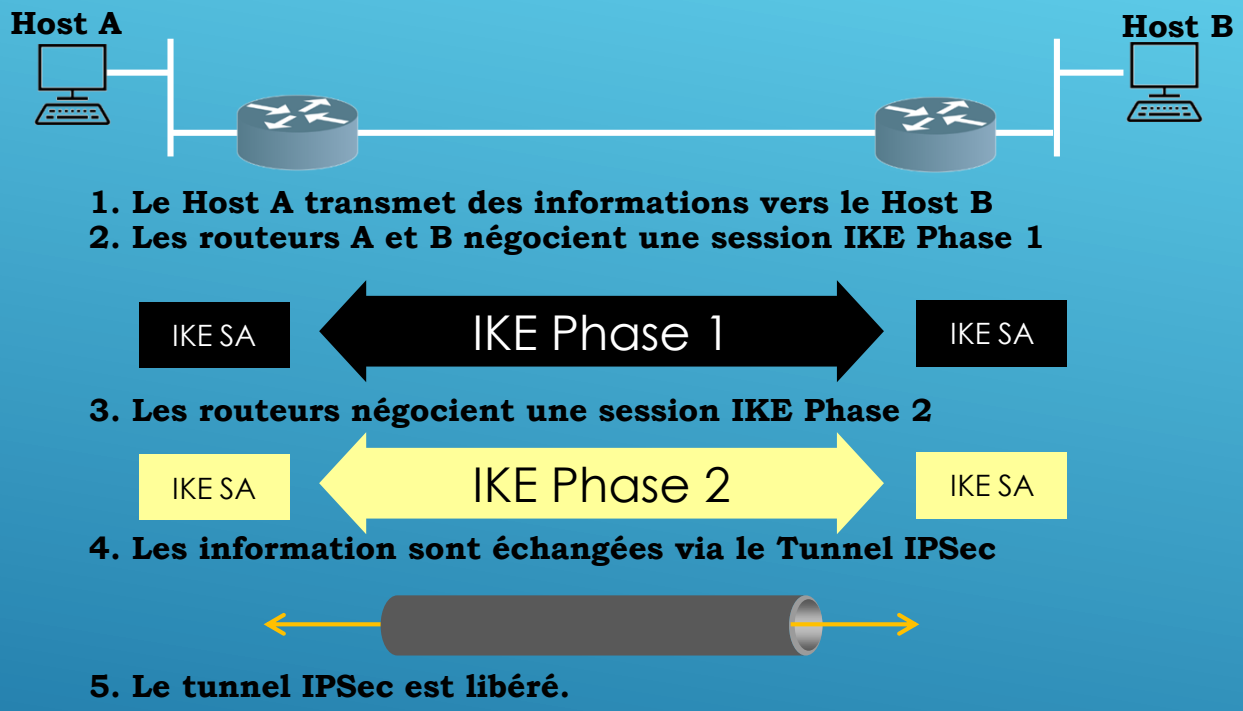
- **Les SAs contiennent des spécifications unidirectionnelles.**
- **les SAs sont spécifiques au protocole d'encapsulation (AH,ESP).**
- **Pour un flux de trafic donné, il y a une SA pour chaque protocole (AH, ESP) et pour chaque sens du trafic.**
- **Les équipements VPN stockent leurs SAs dans une base de données local appelée la SA Database (SADB).**

IPSEC | SECURITY ASSOCIATION (SA)



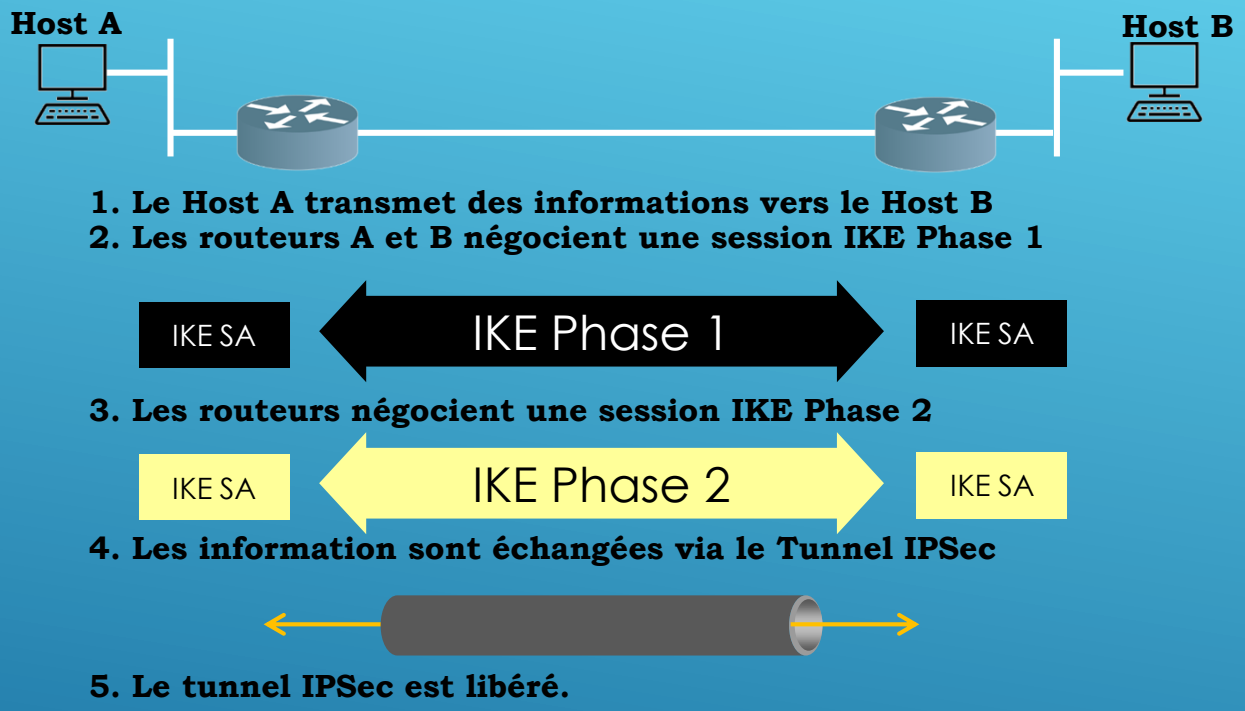
- **Une SA contient les paramètres de sécurité suivants:**
  - **L'algorithme Authentification/Cryptage, longueurs de clés et durées de vie des clés utilisées pour protéger les paquets.**
  - **Les clés de sessions pour l'authentification et le cryptage.**
  - **L'encapsulation IPSec (AH ou ESP) en mode tunnel ou transport.**
  - **Une spécification du trafic réseau auquel s'applique la SA.**

IPSEC | LES CINQ ÉTAPES D'IPSEC



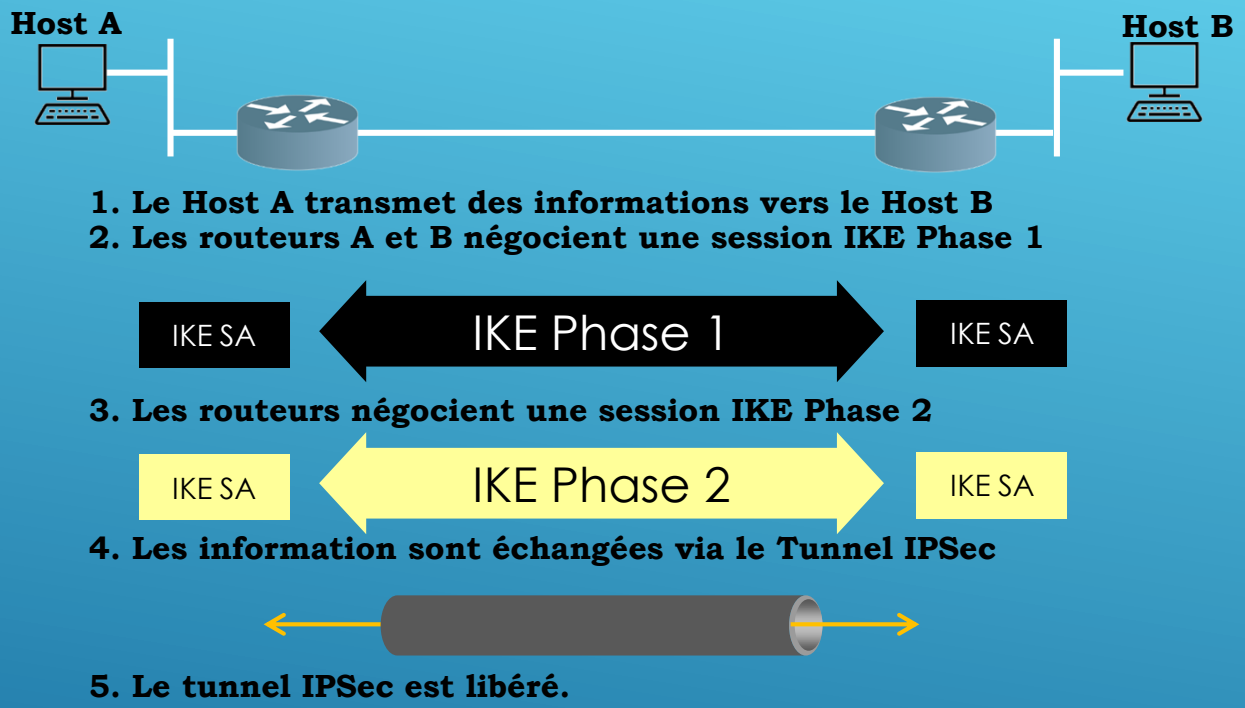
- Le but d'IPSec est de protéger des données avec les moyens de sécurité appropriés
- Le processus IPSec peut être découpé en cinq étapes

IPSEC | LES CINQ ÉTAPES D'IPSEC



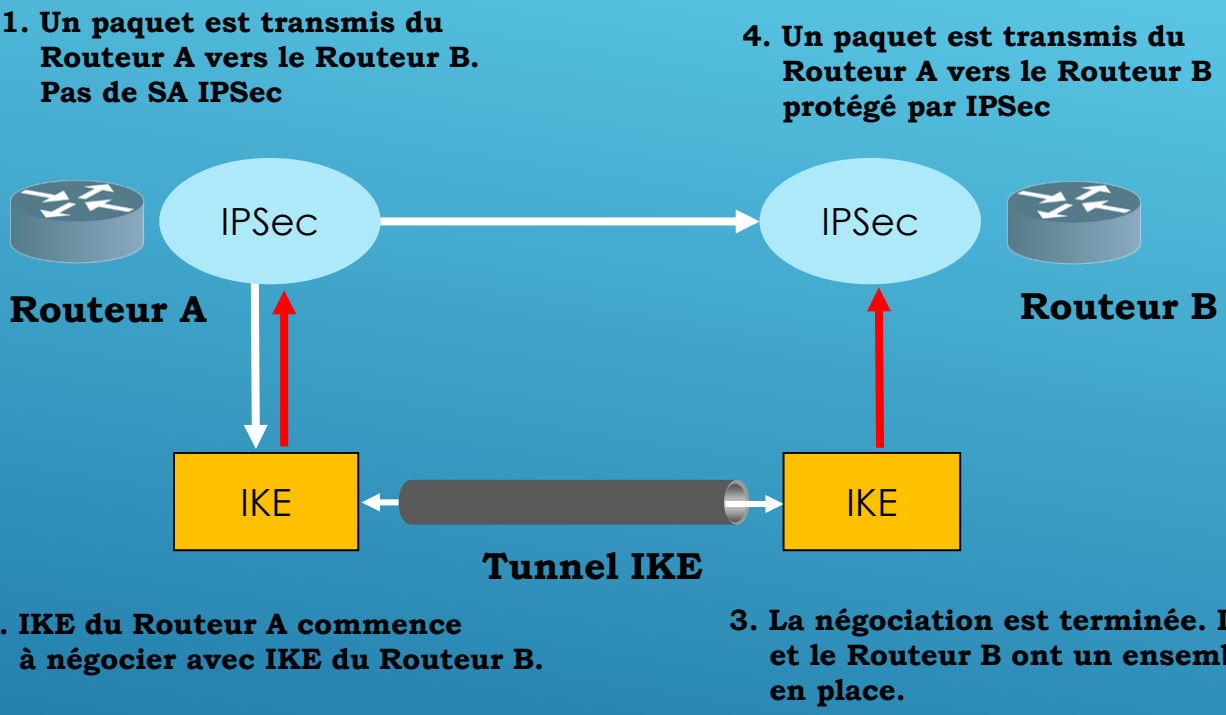
- **Étape 1**
  - Des informations à transmettre initient le processus IPSec
  - Le trafic est dit "intéressant" quand l'équipement VPN reconnaît que les données doivent être protégées.
- **Étape 2**
  - IKE Phase 1 authentifie les extrémités IPSec et négocie les SAs IKE.
  - Ceci crée un canal sécurisé pour négocier les SAs IPSec en Phase 2.

IPSEC | LES CINQ ÉTAPES D'IPSEC



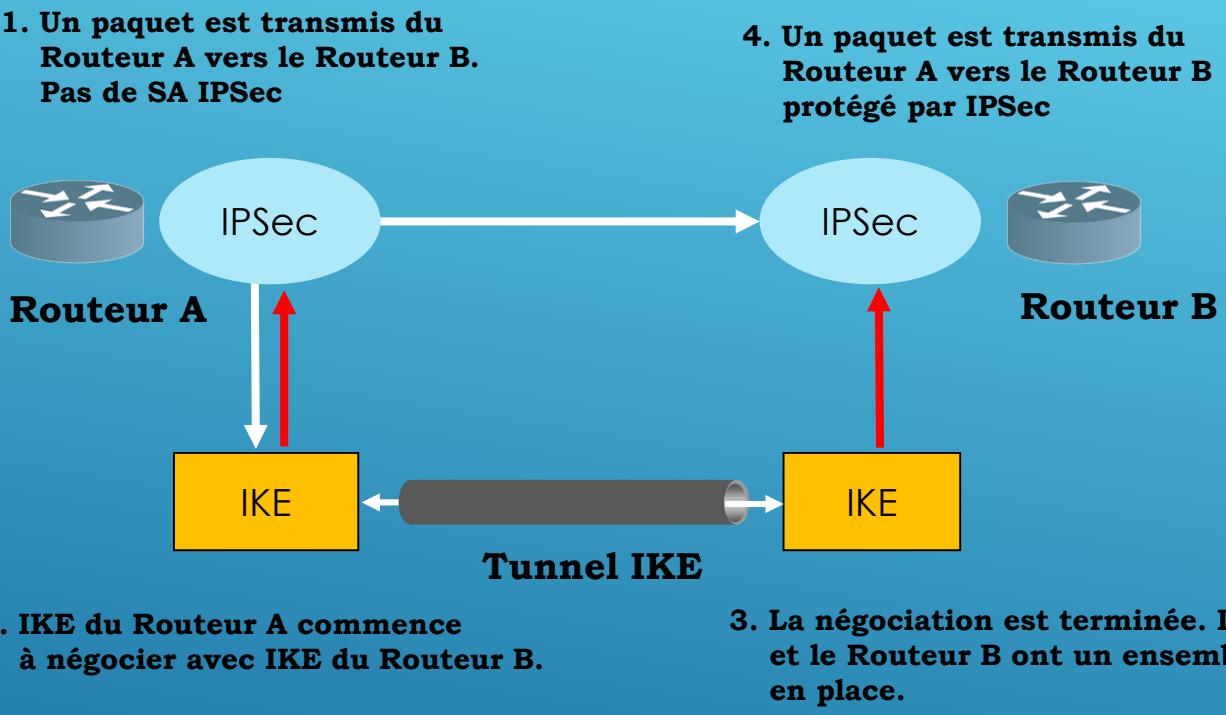
- **Étape 3 :**
  - La phase 2 IKE négocie les paramètres des SAs IPSec et crée une correspondance entre les SAs IPSec des extrémités.
  - Ces paramètres de sécurité sont échangés pour protéger les messages échangés entre les extrémités.
- **Étape 4 :**
  - Le transfert de données est effectué entre les extrémités IPSec sur la base des paramètres IPSEc et des clés stockées dans la base de données SA.
- **Étape 5 :**
  - La libération du tunnel IPSec survient sur effacement au travers des SAs ou sur time out.

IPSEC | COMMENT IPSEC UTILISE IKE



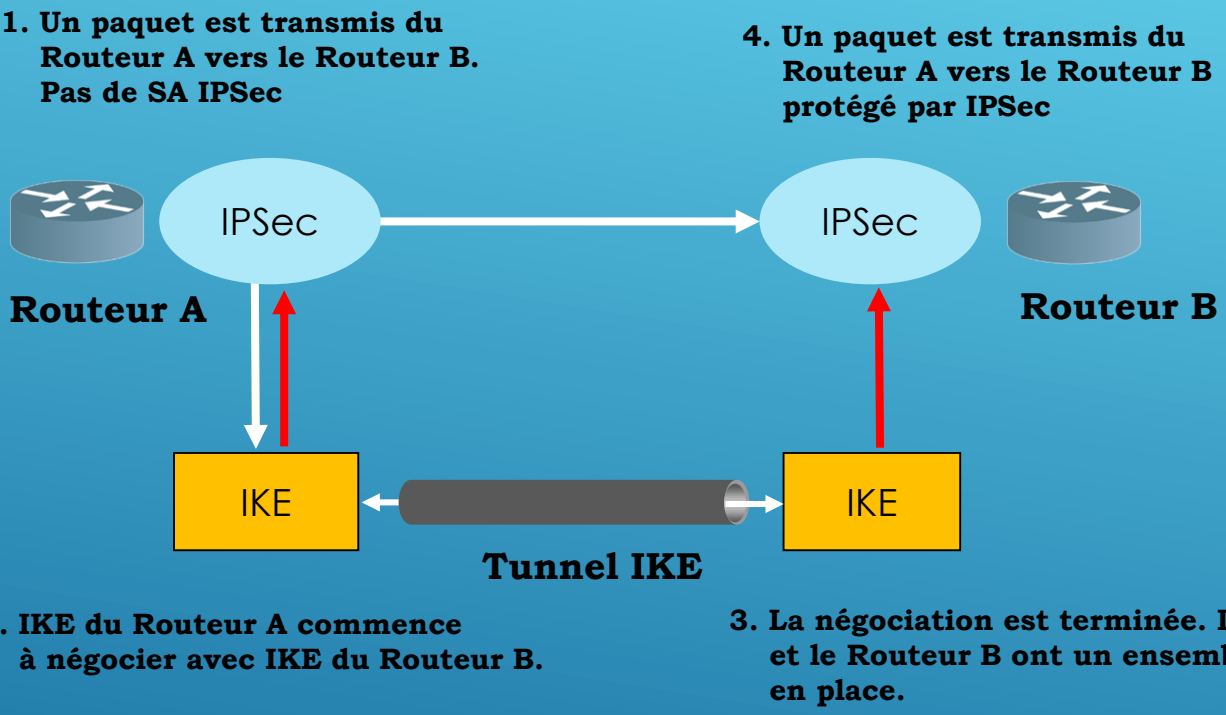
- IKE (Internet Key Exchange) améliore IPSec en fournissant des fonctions additionnelles, flexibilité et facilite la configuration d'IPSec.
- IKE est un protocole hybride qui implémente les échanges de clés Oakley et Skeme dans le cadre ISAKMP (Internet Security Association and Key management)
- IKE fournit l'authentification pour les extrémités IPSec, négocie les clés IPSec et les Associations de Sécurité IPSec

IPSEC | COMMENT IPSEC UTILISE IKE



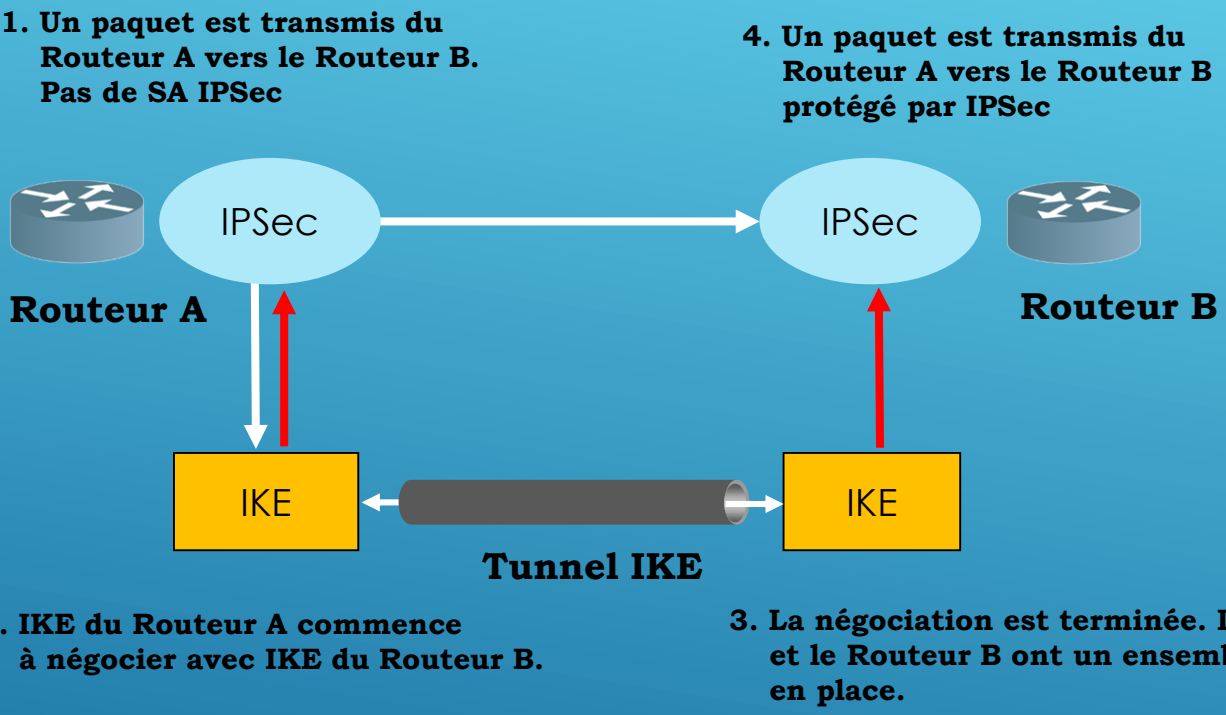
- Le tunnel IKE protège les négociations de SA.
- Le Mode de configuration IKE autorise une passerelle à télécharger une adresse IP vers le client . ceci faisant partie de la négociation IKE.
- L'adresse IP fournie par la passerelle au client IKE est utilisée comme une IP « interne » encapsulée dans IPSec.
- Cette adresse IP connue peut être contrôlée par la politique (policy) IPSec.

IPSEC | COMMENT IPSEC UTILISE IKE



- Le Mode de configuration IKE est implémenté dans les images IOS Cisco « K9 ».
- En utilisant le Mode de configuration IKE, un serveur d'accès Cisco peut être configuré pour télécharger une adresse IP vers un client comme faisant partie de la transaction IKE.
- IKE négocie automatiquement les SAs IPSec et active les communications sécurisées par IPSec sans une pré-configuration manuelle fastidieuse.

IPSEC | COMMENT IPSEC UTILISE IKE

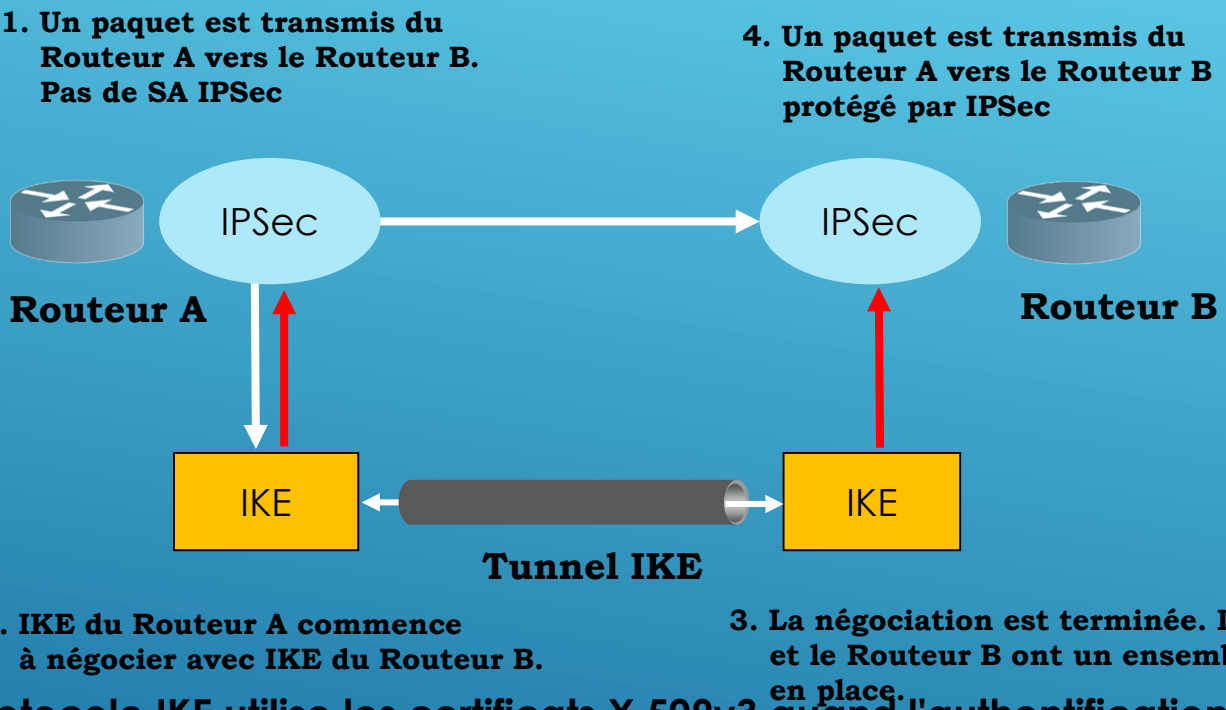


- IKE a les avantages suivants:
  - Élimine la configuration manuelle des paramètres de sécurité IPSec dans des cryptomaps à chaque extrémité.
  - Permet de spécifier une durée de vie pour les SAs.
  - Permet le changement de clés pendant les sessions IPSec.
  - Autorise IPSec à fournir les services de détection d'intrusion d'un tiers.
  - Permet le support d'Autorité de Certification pour une implémentation IPSec évolutive.
  - Permet l'authentification dynamique des extrémités.

IPSEC | COMMENT IPSEC UTILISE IKE

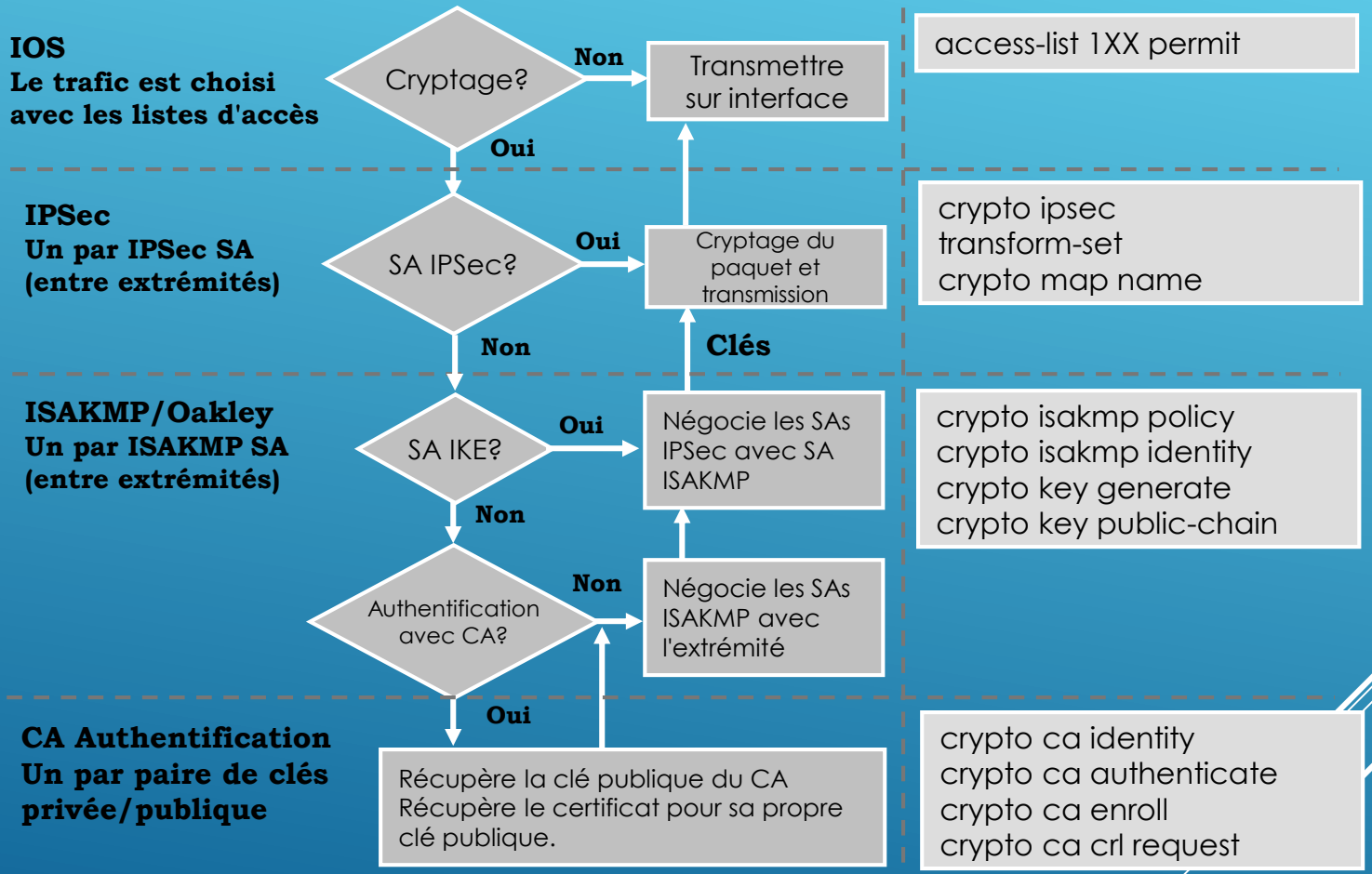
- **Les différentes technologies implémentées pour l'usage d'IKE sont:**
  - **DES (Data Encryption Standard) utilisé pour crypter les données. IKE implémente le standard DES-CBC 56 bits avec Explivit IV (Initialization Vector).**
  - **3DES. Cryptage 168 bits**
  - **CBC (Cipher Bloc Chaining) requiert l'utilisation d'un vecteur d'initialisation (IV). Le vecteur d'initialisation est donné dans le paquet IPSec.**
  - **Diffie-Hellman est un protocol de cryptage à clé publique qui permet à deux parties d'établir un secret partagé sur un canal de communication non-sécurisé. Diffie-Hellman est utilisé dans IKE pour établir les clés de sessions. Les groupes Diffie-Hellman 768-bits et 1024-bits sont supportés.**
  - **MD5 (Message Digest 5), variante HMAC, est un algorithme de hachage utilisé pour authentifier les données. HMAC est une variante qui donne un niveau supplémentaire de hachage.**
  - **SHA (Secure Hash Algorithm), variante HMAC, est un algorithme de hachage utilisé pour authentifier les données. HMAC est une variante qui donne un niveau supplémentaire de hachage.**
  - **Signatures RSA et cryptage RSA. Les signatures RSA fournissent la non-répudiation tandis RSA est utilisé pour le cryptage.**

IPSEC | COMMENT IPSEC UTILISE IKE?



- Le protocole IKE utilise les certificats X.509v3 quand l'authentification requiert des clés publiques.
- Ce support de certificat permet l'évolution du réseau en fournissant l'équivalent d'une carte d'identification numérique à chaque équipement.
- Quand deux équipements veulent communiquer, ils échangent leurs certificats pour prouver leur identité.
- Ceci élimine le besoin d'échanger manuellement des clés publiques avec chaque extrémité ou de spécifier manuellement une clé partagée à chaque extrémité.

IPSEC | COMMENT IPSEC UTILISE IKE?



- **IPSec dans l'IOS Cisco traite les paquets comme le montre la figure ci-dessus**
- **Le processus présume que les clés privées et publiques ont déjà été créees et qu'il existe au moins une liste de controle d'accès.**

IPSEC | COMMENT IPSEC UTILISE IKE?

- Les listes d'accès appliquées à une interface et les crypto map sont utilisées par l'IOS Cisco pour sélectionner le trafic qui doit être protégé (crypté).
- L'IOS Cisco vérifie si les associations de sécurité IPSec (SA) ont été établies.
- Si les SAs ont déjà été établies par configuration manuelle avec les commandes **crypto ipsec transform-set** et **crypto map** ou par IKE, le paquet est crypté sur la base de la "policy" spécifiée dans la crypto map et transmis sur l'interface.
- Si les SAs ne sont pas établies, l'IOS Cisco vérifie si une SA ISAKMP a été configurée et activée.
- Si la SA ISAKMP a été activée, cette SA ISAKMP dirige la négociation de la SA IPSec avec la "policy" ISAKMP configurée par la commande **crypto isakmp policy**.
- Le paquet est crypté par IPSec et transmis sur l'interface.

IPSEC | COMMENT IPSEC UTILISE IKE?

- **Si la SA ISAKMP n'a pas été activée, l'IOS Cisco vérifie si l'autorité de certification a été configurée pour établir une ISAKMP policy.**
- **Si l'authentification de la CA (Certification Authority) a été configurée avec les différentes commandes crypto ca, le routeur utilise les clés publique/privée configurées précédemment, récupère le certificat public de la CA, un certificat pour sa propre clé publique, utilise la pour négocier une SA ISAKMP qui à son tour est utilisée pour négocier une SA IPSEC. Le paquet est crypté puis transmis.**