Sécurité des Réseaux

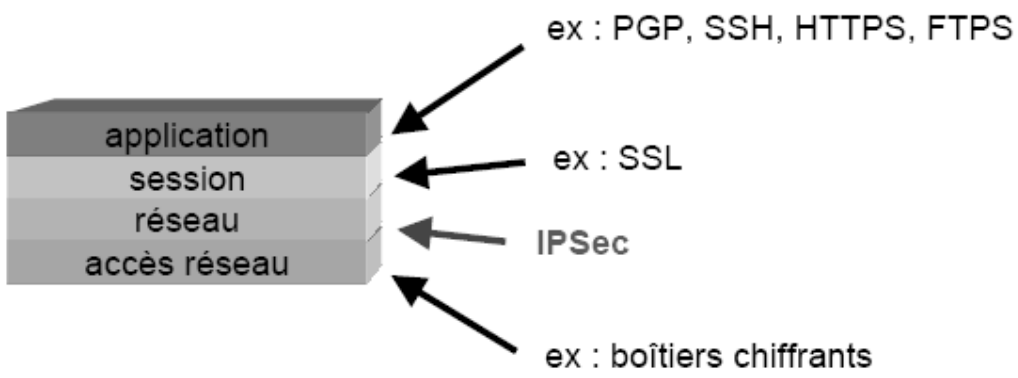
IPSec

Sommaire

- IPSec
  - Les composants
  - Les modes de travail
  - Les associations de sécurité (SA)
    - Combinaisons des SA
  - IPSec - AH
  - IPSec - ESP
  - IPSec - IKE

Où appliquer la sécurité ?

- Pour sécuriser les échanges ayant lieu sur un réseau TCP/IP, il existe plusieurs approches
  - niveau applicatif
  - niveau transport
  - IPsec vise à sécuriser les échanges au niveau de la couche réseau.
  - niveau physique boîtiers chiffrant toutes les données transitant par un lien donné.



IPSec

- Norme IETF (Internet Engineering Task Force) www.ietf.org
  - Première version en 1995
  - Version améliorée avec la gestion dynamique des clés (protocole IKE) en 1998

- Les fonctions de sécurité
  - Confidentialité
  - Intégrité
  - Authentification de l'origine des données
  - Contrôle d'accès
  - Non rejeu

Pourquoi IPSec ?

- IPSec (IP Security) est intégré dans IPv6, ces apports sont:
  - Couche réseau pour le **chiffrement** et **l'authentification**
  - Standards ouverts pour offrir des **communications privées et sécurisées**
  - Solution flexible pour **déployer des politiques de sécurité** à grande échelle

- Statut d'IPSec

- Caractéristiques d'IPSec
  - Solution de sécurité de bout en bout

Les composants d'IPSec

- Il est basé sur plusieurs protocoles, classés en 2 groupes
  - Ceux qui s'appliquent au traitement des paquets
    - Protocoles de sécurité
      - AH (Authentication Header) – authentification et intégrité
      - ESP (Encapsulating Security Payload) – confidentialité et/ou intégrité
    - Protocoles de compression
      - IPCOMP (IP Compression) - la compression
  - Ceux qui concernent la gestion des clés:
    - Le protocole IKE (Internet Key Exchange), s'appuie lui-même sur:
      - Le protocole ISAKMP (Internet Security Association and Key Management Protocol)

Les composants d'IPSec

- Authentication Header **AH** conçu pour assurer l'intégrité et l'authentification des paquets IP sans chiffrement des données

- Encapsulating Security Payload **ESP** a pour rôle premier d'assurer la confidentialité, mais peut aussi assurer l'authenticité des données.

Les composants d'IPSec

- Ces mécanismes peuvent être utilisés seuls ou combinés

- Les mécanismes IPsec ne sont liés à aucun algorithme cryptographique spécifique
  - Les propriétés de l'algorithme utilisé auront un impact sur les fonctions de sécurité fournies.

Les composants d'IPSec

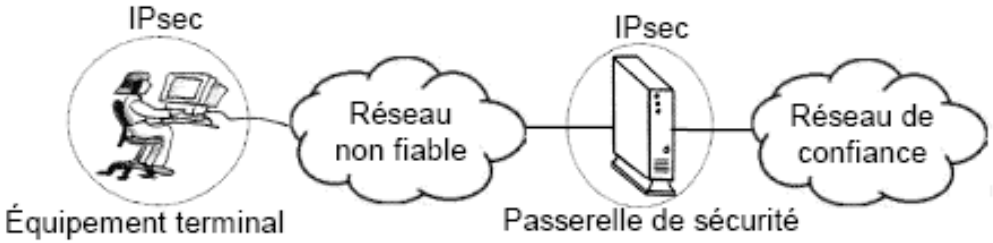
	AH	ESP cryptage	ESP crypt. & auth
Contrôle d'accès	✔	✔	✔
Intégrité des paquets IP	✔		✔
Authentif. de l'origine	✔		✔
Rejet des paquet rejoués	✔	✔	✔
Confidentialité (cryptage)		✔	✔

Types d'utilisations possibles

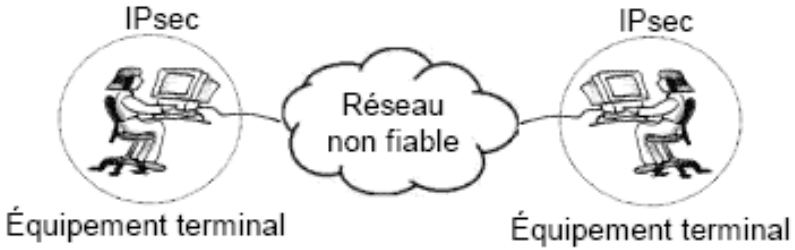
- Trois configurations sont possibles:
  - La première situation est celle où l'on désire relier des réseaux privés distants par l'intermédiaire d'un réseau non fiable (Internet).

Types d'utilisations possibles

- La deuxième situation correspond au cas où l'on désire fournir un accès sécurisé au réseau interne pour des postes nomades.



- Enfin, dans la troisième situation, deux tiers désirent communiquer de façon sécurisée mais n'ont aucune confiance dans le réseau qui les sépare.



Les modes de travail d'IPSec

Le protocole IPSec fonctionne selon 2 modes:

- Transport
  - Protège les données du paquet IP (après l'en-tête IP)
  - Utilisé typiquement en communications ***hôte-hôte ou hôte-serveur***

- Tunnel
  - Protège le paquet IP complet : aucun routeur sur le chemin ne peut examiner l'en-tête IP original
  - IPSec ajoute un en-tête avec des @ source/destination différentes
  - IPSec protège les informations qu'il va transporter
  - Utilisé quand une ou les 2 extrémités du tunnel sont ***des portails sécurisés***

La notion d'association de sécurité

- Les mécanismes mentionnés ci-dessus font appel à la cryptographie
  - Afin de gérer ces paramètres, IPsec a recours à la notion d'association de sécurité Security Association, SA.

- Pour gérer les SA actives, on utilise une «base de données des SA» Security Association Database, SAD.

La notion d'association de sécurité

- Une SA est unidirectionnelle
  - Les services de sécurité sont fournis par l'utilisation de AH ou de ESP.
  - Si AH et ESP sont tous deux appliqués au trafic en question, on parle alors de paquet (bundle) de SA.

- Chaque SA est identifiée de manière unique à l'aide d'un triplet composé de
  - L'adresse de destination des paquets.
  - L'identifiant du protocole de sécurité utilisé (AH ou ESP).
  - Un index des paramètres de sécurité (Security Parameter Index) SPI (bloc de 32 bits)

Les associations de sécurité
Les paramètres de la SA (1)

- **SPI**
- **L'adresse IP de la source** et celle de la **destination**
- **Le nom**
- Le **protocole de sécurité**
- Les **paramètres d'authentification**
- Le **mode**: Transport ou Tunnel
- Les **protections contre la réplication**
  - Le compteur de séquences
  - L'indicateur de dépassement de séquence.

Les associations de sécurité
Les paramètres de la SA (2)

- **La durée de vie de la SA** indiquée en unités de temps ou en nombres d'octets traités
  - Quand une SA expire, les paquets qui lui sont associés sont généralement détruits jusqu'à ce qu'une nouvelle SA soit négociée.

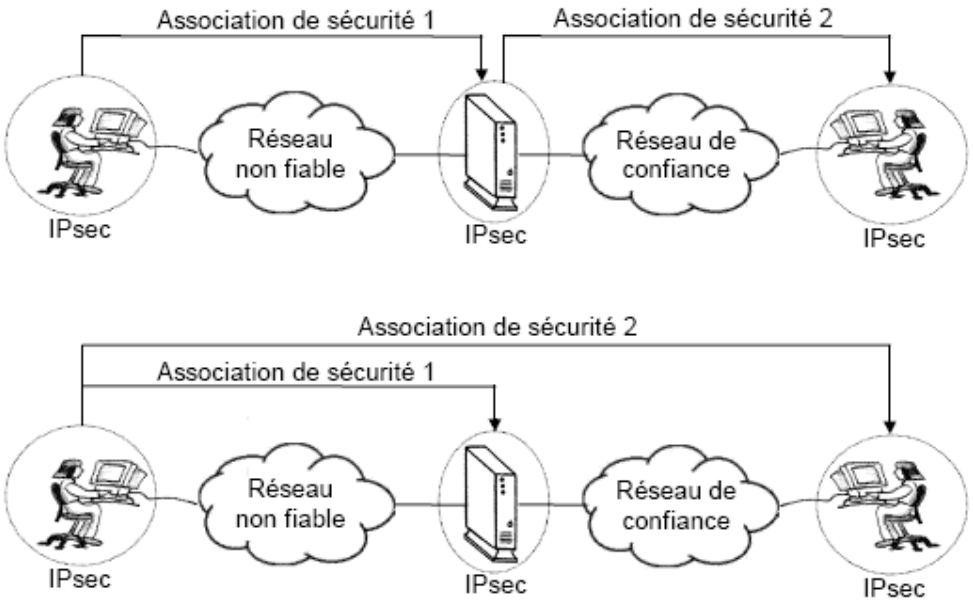
- **Les paramètres de fragmentation (PMTU)**

Les associations de sécurité

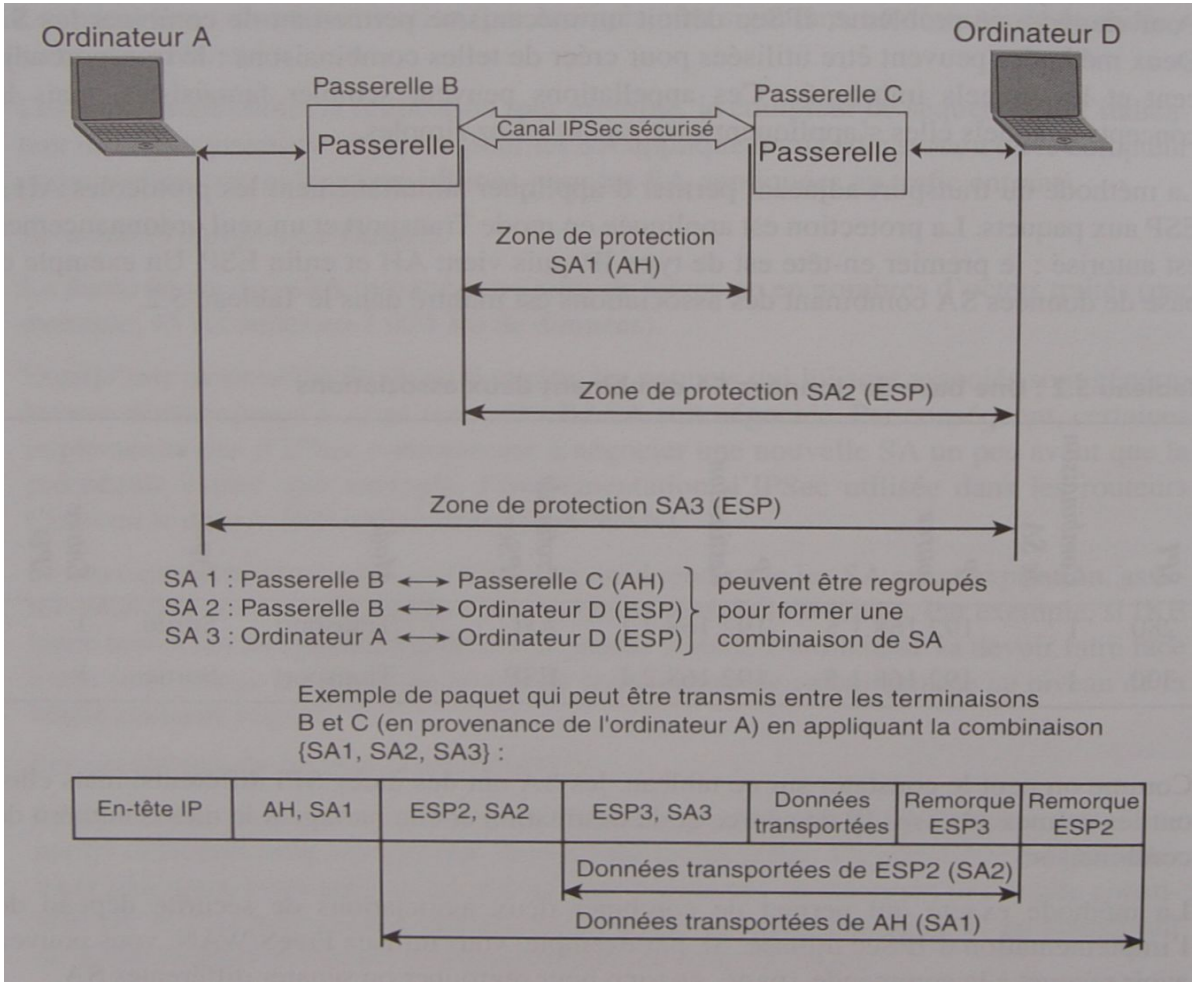
- IPSec définit 2 méthodes permettant de combiner les SA
  - Le transport adjacent
    - Permet d'appliquer simultanément AH et ESP aux paquets.
  - Les tunnels imbriqués
    - Permet de regrouper autant d'en-têtes AH ou ESP qu'on veut.

Les associations de sécurité

- Des configurations plus complexes où plusieurs associations de sécurité se succéderaient ou se superposeraient partiellement :



Tunnels imbriqués



La gestion des clefs et SAs

- La gestion des clefs pour IPsec n'est liée aux autres mécanismes de sécurité IPsec que par le biais des SAs.
  - La règle générale est d'utiliser un protocole spécifique qui permet la négociation dynamique des SA et l'échange des clefs de session.

- IPv6 n'est pas destiné à supporter une gestion des clefs "en bande"
  - Découplage clair du mécanisme de gestion des clefs et des autres mécanismes de sécurité.

La gestion des clefs et SAs

- Le protocole de négociation des SAs développé pour IPsec s'appelle « protocole de gestion des clefs et des associations de sécurité pour Internet », ISAKMP.

- ISAKMP est en fait inutilisable seul
  - Dans le cadre de la standardisation de IPsec, ISAKMP est lié en partie à d'autres protocoles (SKEME et Oakley) pour donner un protocole final du nom d'IKE « Internet Key Exchange ».

Politique de sécurité: SPD

- Sur chaque système capable d'utiliser IPsec doit être présente une SPD (Security Policy Database)
- Chaque entrée de cette BdD est identifiée par un SPI unique choisi arbitrairement.
  - Elle sert a préciser les services de sécurité, les protocoles et les algorithmes à utiliser.
- Trois choix de traitement pour un paquet IP sont possibles:
  - rejeter le paquet
  - laisser passer le paquet sans protection IPSec
  - laisser passer le paquet avec une protection IPSec
- On définit l'ensemble du trafic grâce à des sélecteurs qui définissent la granularité des SA:
  - @ IP destination et @ IP source
  - nom (d'utilisateur ou de système)
  - protocole de la couche transport
  - ports source et destination

Politique de sécurité: SAD

- La SAD contient les paramètres de chaque SA active:
  - Compteur de numéro de séquence (SNC, Sequence Number Counter)
  - Algorithme d'authentification d'AH
  - Algorithme de chiffrement (et d'intégrité éventuellement) d'ESP
  - Durée de vie de la SA

Politique de sécurité

Principe de fonctionnement :

- On distingue deux situations :
  - Trafic sortant :
    - Quand la « couche IPsec » reçoit des données à envoyer, elle commence par consulter la SPD pour savoir comment traiter ces données.
    - Si cette base lui indique que le trafic doit se voir appliquer des mécanismes de sécurité, elle récupère les caractéristiques requises pour la SA correspondante et va consulter la base des SA, la SAD.
    - Si la SA nécessaire existe déjà, elle est utilisée pour traiter le trafic en question.
    - Dans le cas contraire, IPsec fait appel à IKE pour établir une nouvelle SA avec les caractéristiques requises.

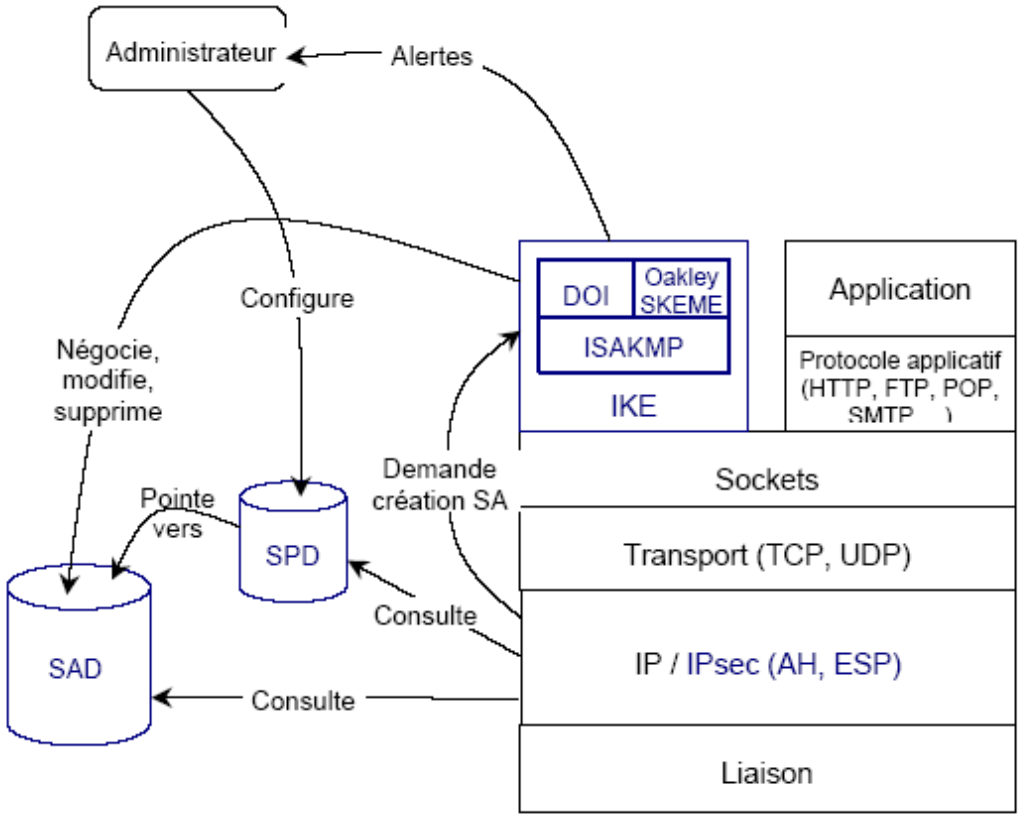
Politique de sécurité

Principe de fonctionnement :

- On distingue deux situations :
  - Trafic entrant :
    - Quand la couche IPsec reçoit un paquet en provenance du réseau, elle examine l'en-tête pour savoir si ce paquet s'est vu appliquer un ou plusieurs services IPsec et si oui quelles sont les références de la SA.
    - Elle consulte alors la SAD pour connaître les paramètres à utiliser pour la vérification et/ou le déchiffrement du paquet.
    - Une fois le paquet est vérifié et/ou déchiffré, la SPD est consultée pour savoir si l'association de sécurité appliquée au paquet correspondait bien à celle requise par la politique de sécurité.

Politique de sécurité

Principe de fonctionnement :



Authentication Header AH

- RFC 2402 (novembre 1998), AH assure :
  - Intégrité des données en mode non connecté
  - Authentification de l'origine des données
  - Protection contre le rejeu (optionnelle)
- L'absence de confidentialité dans AH permet de s'assurer que ce standard pourra être largement répandu sur l'Internet

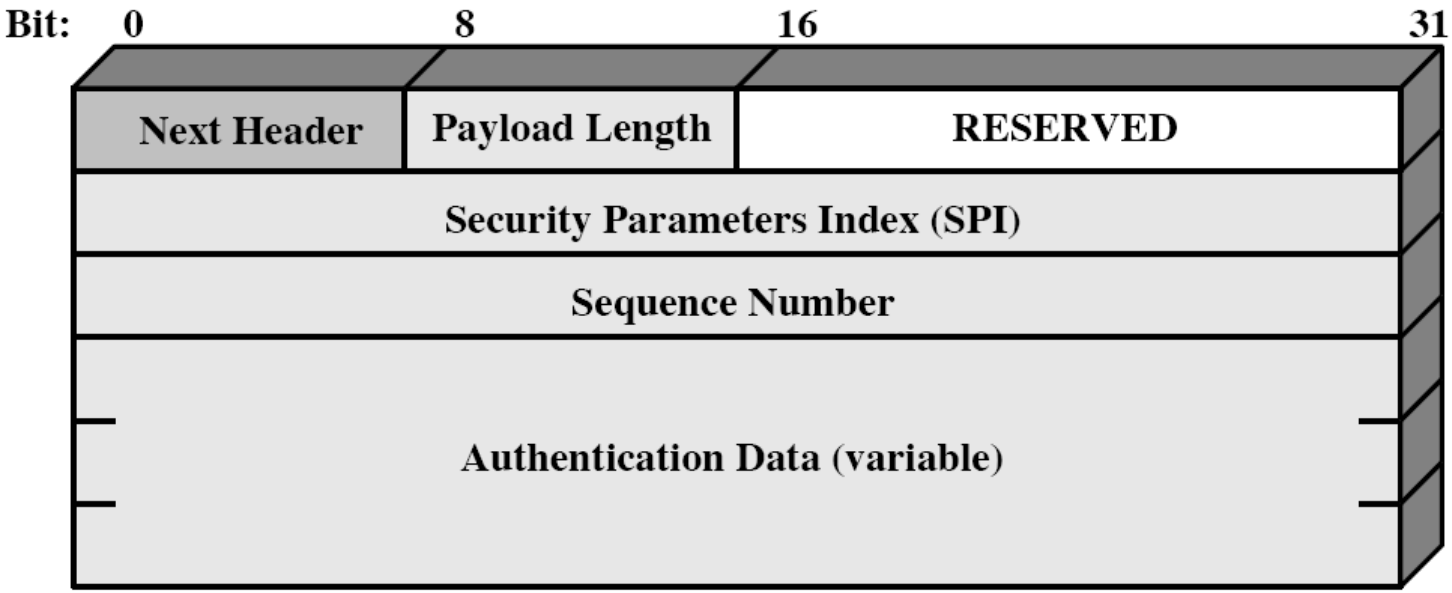
Authentication Header AH

- Intégrité et authentification sont fournies ensemble, à l'aide d'un bloc de données supplémentaire adjoint au message à protéger.
  - Ce bloc de données est appelé « valeur de vérification d'intégrité » Integrity Check Value, ICV

- La protection contre le rejeu se fait grâce à un numéro de séquence; elle n'est disponible que si IKE est utilisé

IPSec Authentication Header

- Rôle d'authentification
  - des données (mode transport)
  - des données et de l'en-tête (mode tunnel)



IPSec Authentication Header

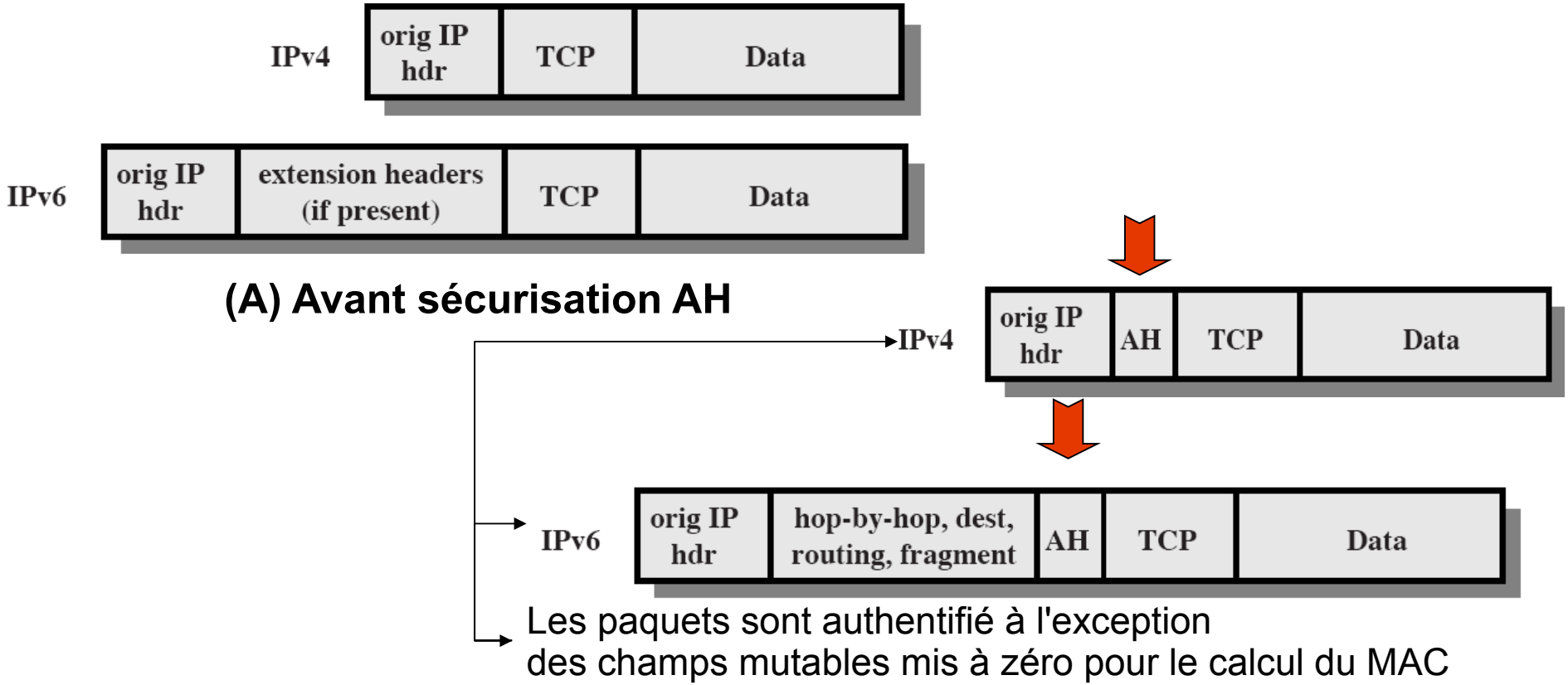
- Next Header: protocole de niveau supérieur (TCP: 6, UDP: 7)
- Payload Length : longueur du bloc AH.
- RESERVED : emplacement réservé pour le futur.
  - Tous les bits doivent être mis à 0.
- SPI : identifiant unique de l'association de sécurité.
- Sequence Number Field : protection contre le rejeu (index initialisé à 0).

IPSec Authentication Header

- Authentication Data (résultat du hachage signé)
  - L'expéditeur calcule les données d'authentification à partir de l'ensemble des champs invariants du datagramme IP final, y compris AH
  - Les champs variables et le champ destiné à recevoir les données d'authentification sont considérés comme égaux à zéro pour le calcul.
  - Le récepteur vérifie l'exactitude de ces données à la réception.

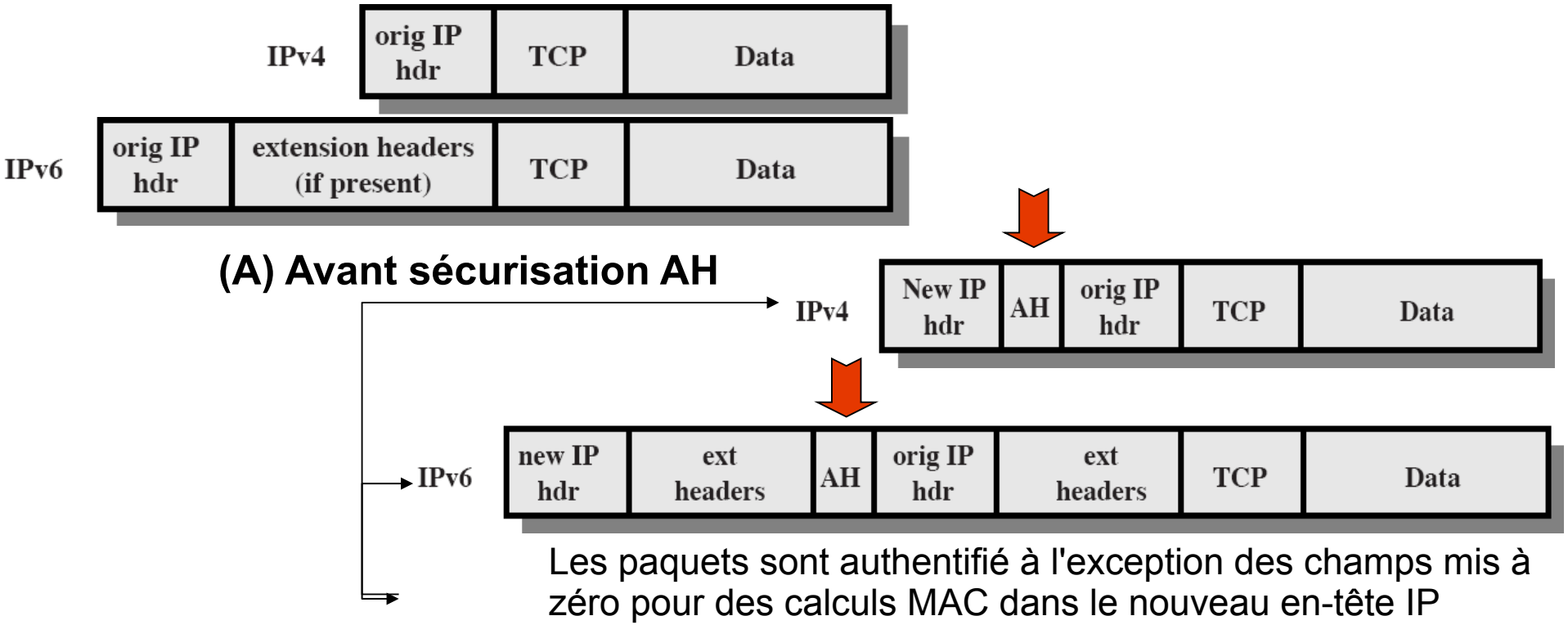
Les modes de travail d'IPSec

- Mode Transport: conservation de l'en-tête d'origine



Les modes de travail d'IPSec

- Mode Tunnel: IPSec traite la totalité du paquet comme un bloc de données: ajout d'un nouvel entête



Encapsulating Security Payloard (ESP)

- RFC 2406, ESP peut assurer au choix:
  - Confidentialité:
    - Confidentialité des données
  - Intégrité des données, authentification de l'origine des données et protection contre le rejeu.

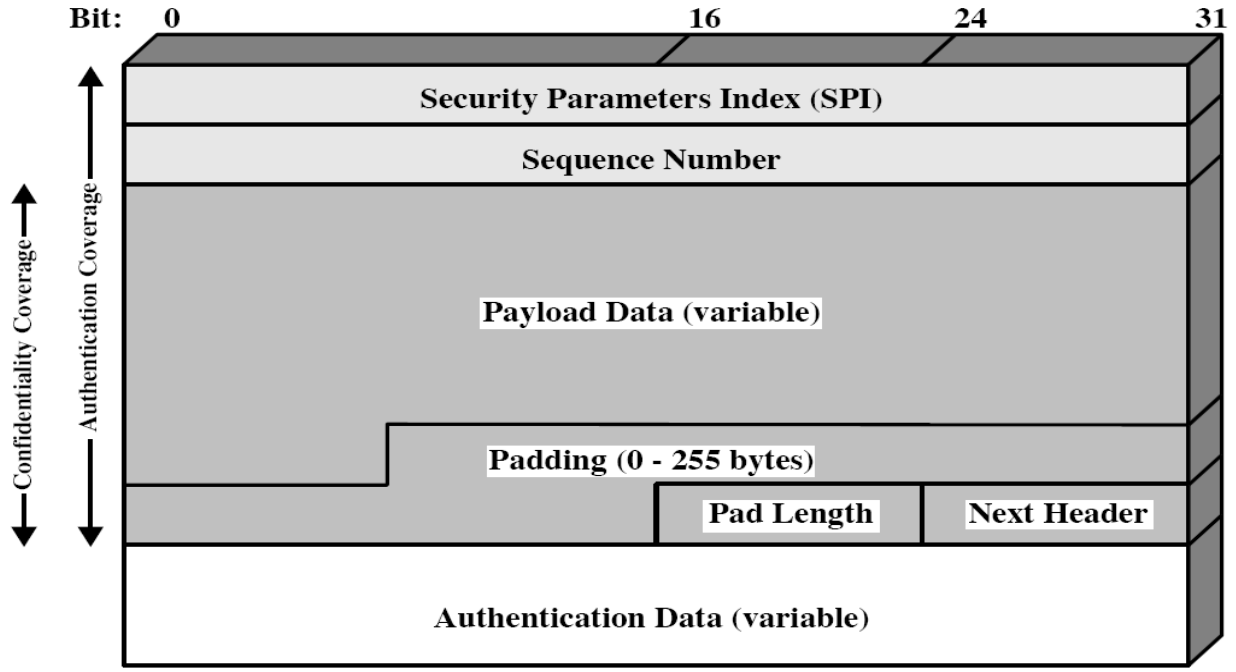
Encapsulating Security Payloard (ESP)

- La protection contre le rejeu ne peut être sélectionnée que si l'intégrité l'a été et que IKE est utilisé.

- ESP fonctionne suivant le principe de l'encapsulation:
  - Les données originales sont chiffrées puis encapsulées entre un header et un trailer.

IPSec Encapsulating Security Payloard (ESP)

- Rôle : Cryptage et (éventuellement)
  - authentification des données (mode transport)
  - authentification des données + en-tête (mode tunnel)

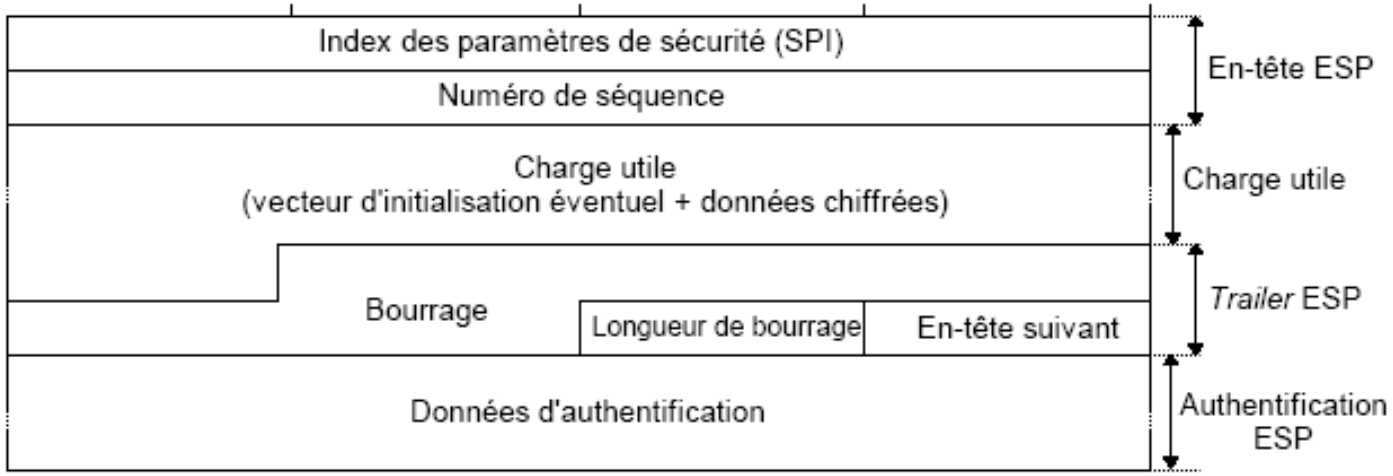


IPSec Encapsulating Security Payloard (ESP)

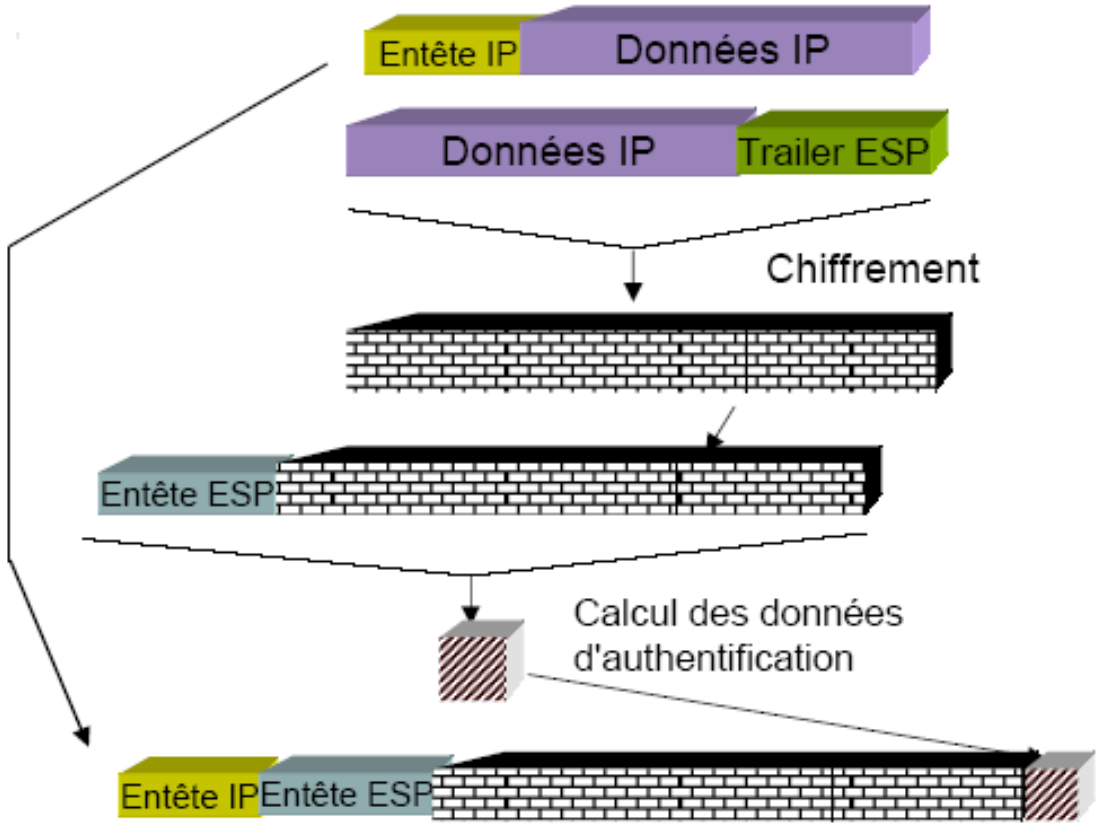
- SPI : identifiant unique de la SA (comme pour AH).
- Sequence Number Field : protection contre le rejeu (index initialisé à 0).
  - Comme pour AH, l'émetteur l'active obligatoirement.
  - Le récepteur choisit de prendre ce champ en compte ou non.
- Payload Data : contient les données chiffrées.
- Next Header : protocole de niveau supérieur (TCP, UDP, ...)
- Authentication Data : données d'authentification du paquet ESP. Ce champ n'authentifie pas l'en-tête IP

IPSec Encapsulating Security Payloard (ESP)

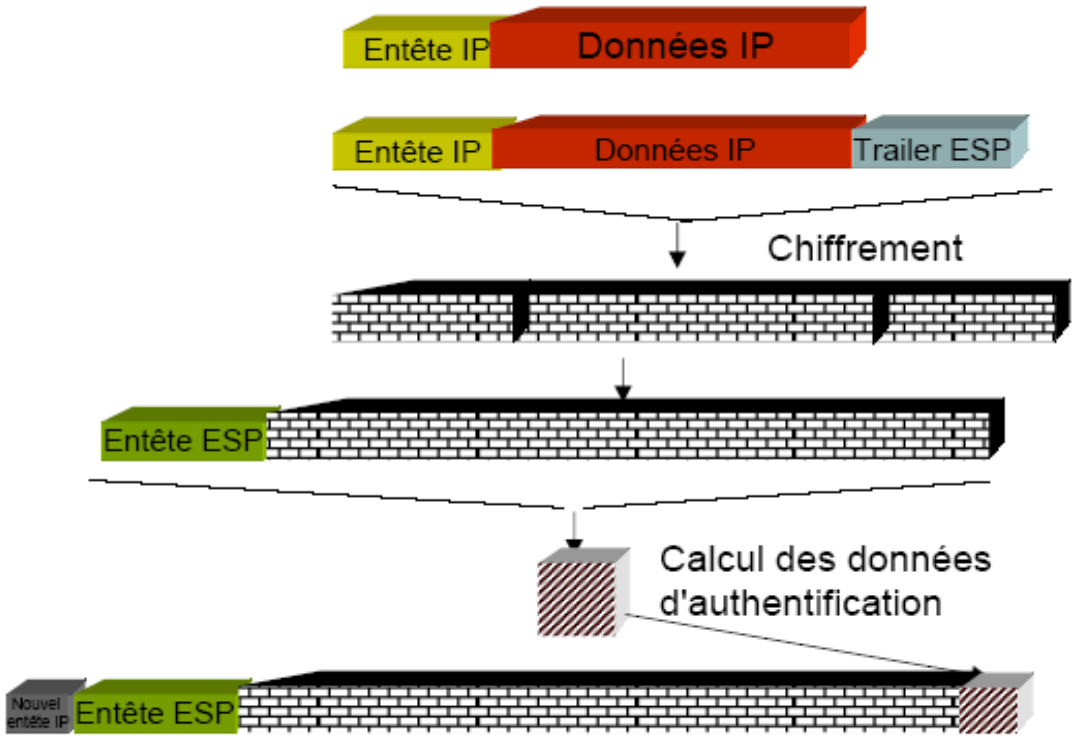
- Le champ bourrage peut être nécessaire pour les algorithmes de chiffrement par blocs.
- Les données d'authentification ne sont présentes que si ce service a été sélectionné.



IPSec ESP - mode Transport

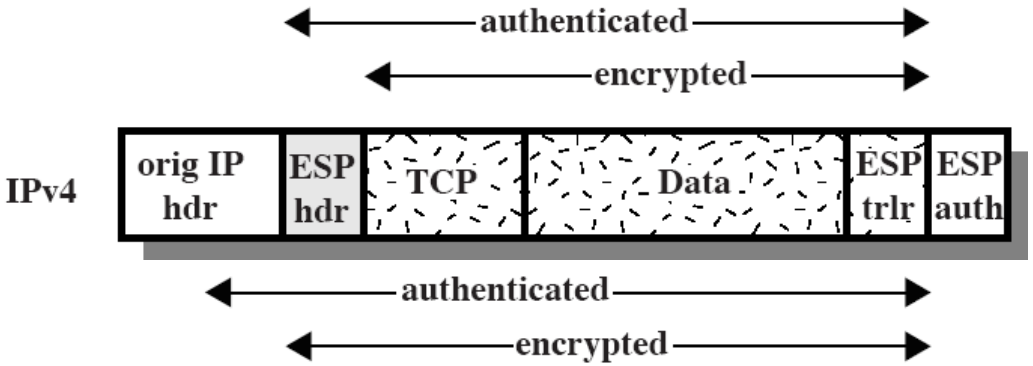


IPSec ESP - mode Tunnel

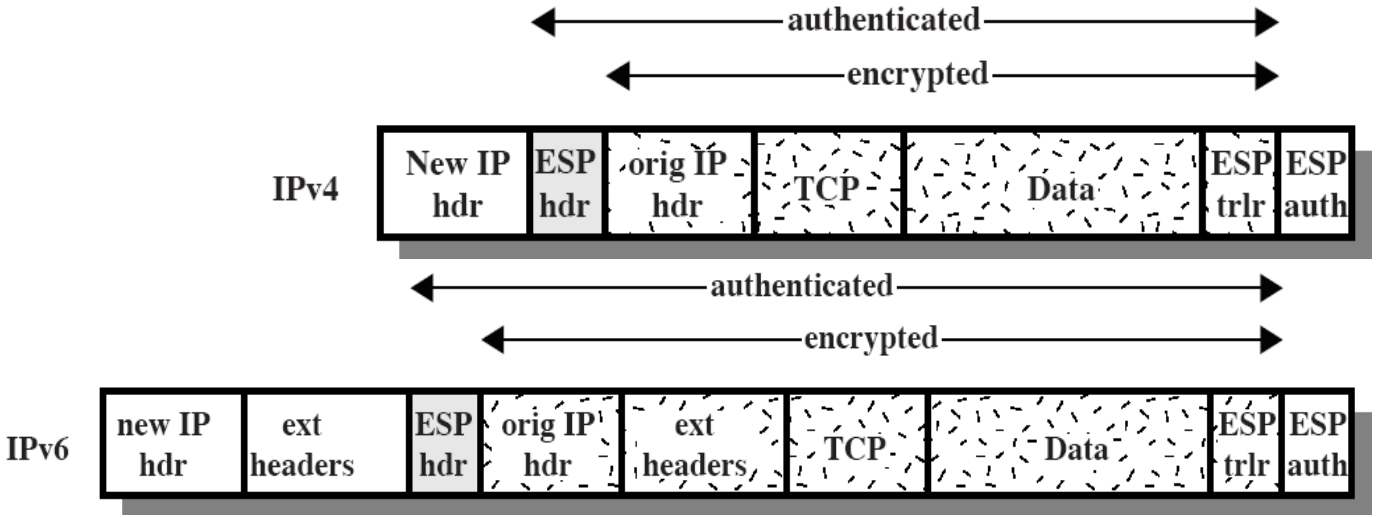


IPSec ESP - mode Transport et Tunnel

- Mode Transport



- Mode Tunnel



AH et ESP

- AH seul
  - Authentification poussée, garantie d'intégrité et protection contre la duplication.
- ESP seul
  - Authentification (optionnelle), garantie d'intégrité, protection contre la duplication et chiffrement du contenu
- ESP et AH
  - Authentification poussée, garantie d'intégrité, protection contre la duplication et chiffrement du contenu.
- ESP et IPCOMP
  - Authentification, garantie d'intégrité, protection contre la duplication, chiffrement du contenu et compression
- ESP, AH, et IPCOMP.
  - Authentification poussée, garantie d'intégrité, protection contre la duplication, chiffrement du contenu et compression

Problèmes divers

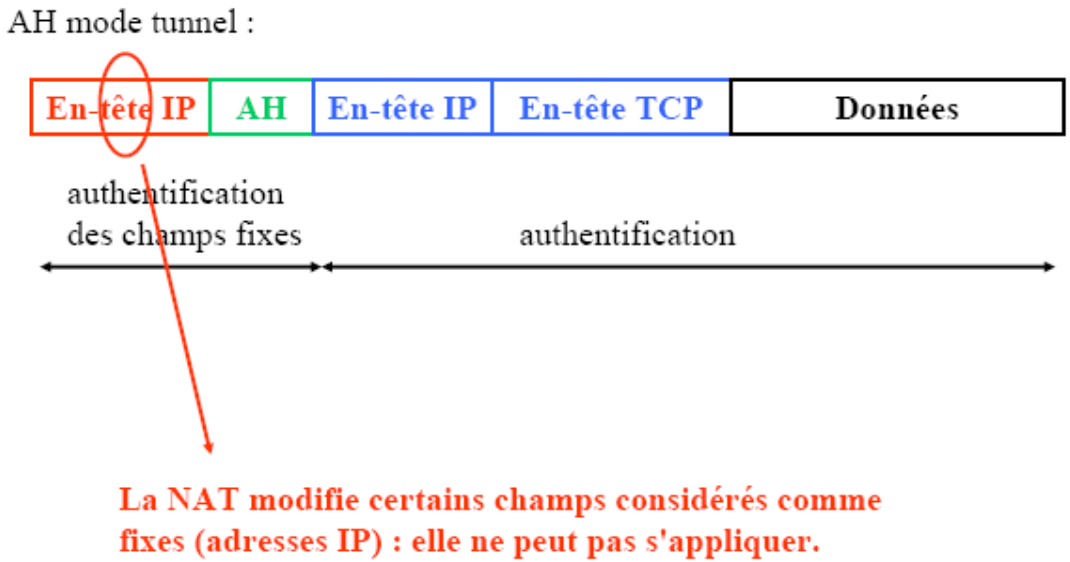
1. Limitations dues à la gestion manuelle des clefs
- Les services d'unicité offerts par AH et ESP s'appuient sur des numéros de séquence initialisés à 0 lors de la création d'une SA et incrémentés lors de l'envoi de chaque datagramme.

2. Broadcast et multicast

3. Firewalls
- Le filtrage de datagrammes IPsec est délicat

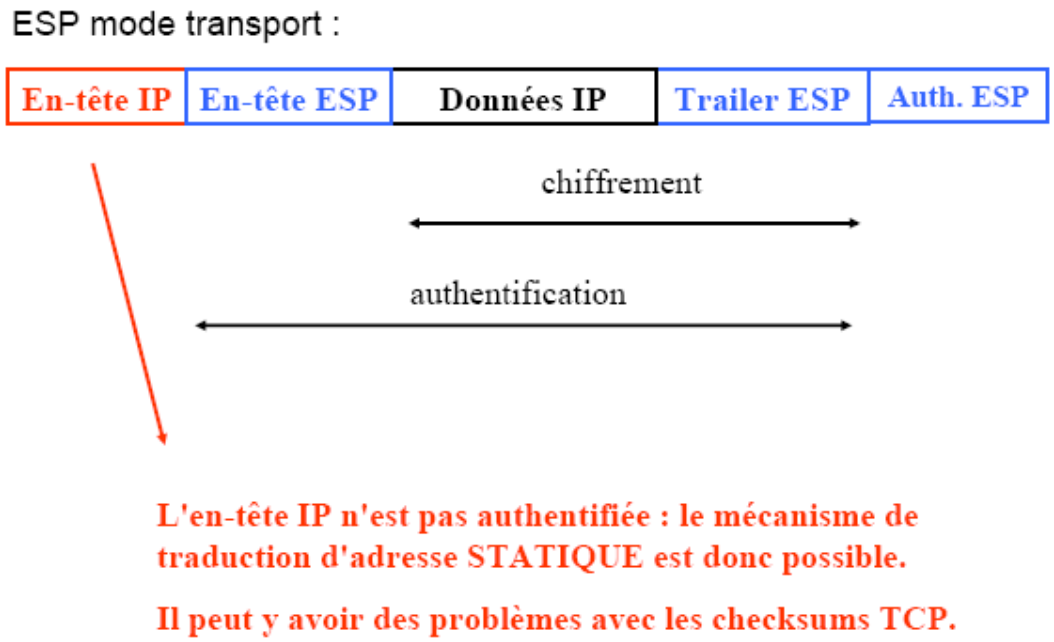
Problèmes divers

4. NATs



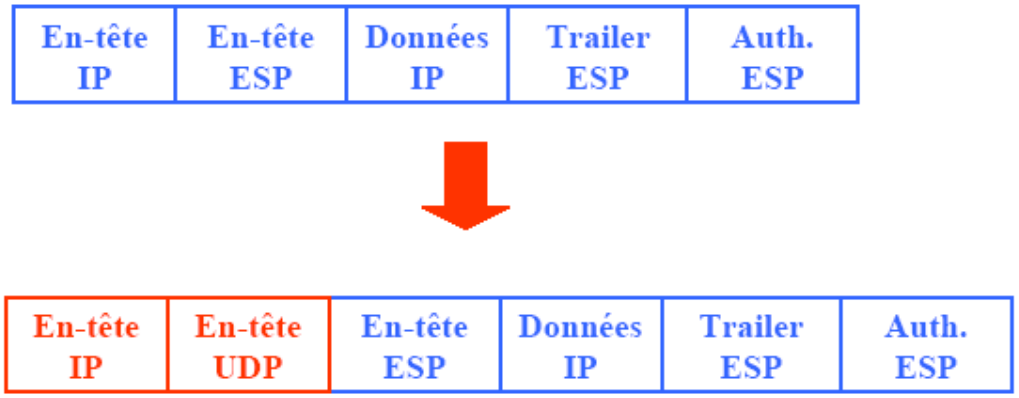
Problèmes divers

4. NATs (suite)



Problèmes divers

4. NATs (suite)
   - Une solution pour utiliser la NAT est d'encapsuler IPSec sur de l'UDP :



Problèmes divers

5. Protocoles autres qu'IP
   - Un inconvénient d'IPsec est que ce protocole ne prévoit que le convoyage sécurisé de datagrammes IP.

Echange de clefs et authentification

- Une connexion sécurisée comporte des opérations de cryptographie à clés publiques complexes.
  - Il faut donc réaliser cette opération le plus rarement possible et réutiliser tous les paramètres rémanents dans un contexte partagé par plusieurs connexions TCP.

Echange de clefs et authentification

- Ce contexte doit avoir un nom et être connu des 2 entités communicantes.
  - Ceci revient à créer une connexion dans une couche supérieure à la couche Transport.

- Il existe deux couches qui peuvent être le point de gestion de ce contexte : la couche Session 6 et la couche Application 7.
  - SSL/TLS, dédié à la sécurisation de TCP utilise la première solution.

Echange de clefs et authentification

Propriétés des protocoles d'échange de clef

- DIFFIE, VAN OORSCHOT et WIENER définissent la notion de protocole d'authentification mutuelle avec échange de clef sûr. Un protocole est dit sûr si les deux conditions suivantes sont valables:
  - Les enregistrements des messages échangés par les deux tiers se correspondent.
  - Il est matériellement impossible pour toute personne autre que les tiers en présence de retrouver la clef échangée.

- D'autres propriétés des protocoles d'échange de clef peuvent être souhaitables :
  - **Perfect Forward Secrecy** PFS.
    - Généralement, cette propriété assure également que la découverte d'une clef de session ne compromet ni les secrets à long terme ni les autres clefs de session.

Echange de clefs et authentification

Propriétés des protocoles d'échange de clef

- **Back Traffic Protection** est fournie si la génération de chaque clef de session se fait de manière indépendante
- **Authentification directe** (Direct Authentication)
- **Protection de l'identité** (Identity Protection)
- L'utilisation du temps **Timestamps** afin d'éviter le rejeu
  - Méthode très controversée du fait de sa trop grande dépendance d'horloges synchronisées.

Echange de clefs et authentification

Propriétés des protocoles d'échange de clef

- Dans DIFFIE-HELLMAN, une façon de contourner le problème de l'attaque de l'intercepteur est d'authentifier les valeurs publiques utilisées pour la génération du secret partagé.
  - Méthode du protocole SKIP, du protocole Photuris

- Perte de la possibilité de générer un secret partagé sans aucune information préalable sur l'interlocuteur.

Echange de clefs et authentification

Les protocoles d'authentification mutuelle avec échange de clef développés pour IP

- Il existe de nombreux protocoles d'authentification mutuelle avec échange de clef selon leurs pré-requis et leurs propriétés
- Pour IP, une distinction supplémentaire s'impose entre les protocoles orientés connexion et ceux sans connexion.

Echange de clefs et authentification
SKIP

- SKIP (Simple Key management for Internet Protocols) ne se base pas sur l'établissement d'une « connexion »
  - SKIP se base sur une génération de secret partagé DIFFIE-HELLMAN avec valeurs publiques authentifiées.

- Historique: créé en 1994 par SUN MICROSYSTEMS. SKIP fut proposé comme protocole de gestion des clefs standard pour IPsec, mais c'est ISAKMP/Oakley qui fut choisi en septembre 1996.

Echange de clefs et authentification
SKIP

- Echange de clefs:
  - Pour implémenter SKIP, chaque tiers doit posséder une valeur publique DIFFIE-HELLMAN authentifiée.
  - Pour communiquer avec un interlocuteur choisi, un tiers doit obtenir sa valeur publique.
  - g^a mod p et g^b mod p sont les valeurs publiques, a et b les valeurs privées et (g^a)^b mod p le secret partagé à long terme et sert à dériver une clef secrète Kab.

- Utilisation des clefs:
  - Kab est en fait une clef de chiffrement de clef utilisée pour chiffrer une clef Kp, appelée clef de paquet, qui est elle-même utilisée pour générer deux clefs, servant au chiffrement et à l'authentification d'un paquet IP

Echange de clefs et authentification
SKIP

- Extension pour la propriété de PFS
  - Une extension de SKIP garantissant cette propriété a donc été développée
    - Une génération de clefs DIFFIE-HELLMAN éphémère, car reposant sur des valeurs publiques à court terme.
  - L'utilisation d'une génération de clefs DIFFIE-HELLMAN éphémère implique l'échange de certificats contenant les valeurs publiques correspondantes.

Echange de clefs et authentification
Photuris

- Créé en 1995 par Qualcomm et DayDreamer.
- Photuris est un protocole «orienté connexion»
  - Photuris s'est vu attribué le port UDP 468 par l'IANA.
- Principe:
  - Basé sur la génération d'un secret partagé selon le principe de DIFFIE-HELLMAN.

Echange de clefs et authentification
Photuris

- Principe (suite):
  - Afin de contrer l'attaque de « Man in the middle », l'échange des valeurs servant à générer le secret partagé est suivi d'une authentification.

  - Un problème de DIFFIE-HELLMAN est que ce protocole requiert des opérations coûteuses en ressources système, ce qui le rend vulnérable à des attaques de déni de service appelées «attaques par inondation».

Echange de clefs et authentification
Photuris

- Le protocole Photuris est composé des 3 étapes suivantes :
  1. Cookie exchange
  2. Value exchange
  3. Identity exchange

- En parallèle de ces échanges, les tiers se mettent d'accord sur:
  - La méthode de génération du secret partagé
  - Certains paramètres de sécurité utiles à la SA mise en place.

Echange de clefs et authentification
SKEME

- Développé spécifiquement pour IPsec, SKEME est une extension de Photuris proposée en 1996 par IBM.
  - SKEME fournit divers modes d'échange de clef.

- Principe
  - Le mode de base de SKEME repose sur l'utilisation de clefs publiques et sur une génération de secret partagé D-H.
  - Mais SKEME permet également l'utilisation d'une clef précédemment partagée.

Echange de clefs et authentification SKEME

- Principe (suite)
  - En résumé, SKEME comporte quatre modes distincts:
    1. Le mode de base
    2. Un échange de clef basé sur l'utilisation de clefs publiques, mais sans D-H.
    3. Un échange de clef basé sur l'utilisation d'une clef partagée précédemment et sur D-H.
    4. Un mécanisme de changement de clef rapide basé uniquement sur des algorithmes symétriques.

Echange de clefs et authentification SKEME

- Principe (suite)
  - SKEME se décompose en 3 phases:
    - SHARE,
    - EXCH,
    - AUTH.
  - Une autre phase, dite phase COOKIES, peut être ajoutée avant la phase SHARE afin de protéger contre les attaques en déni de service en ayant recours au mécanisme des cookies.

Echange de clefs et authentification
Oakley

- Initialement proposé par l'université d'Arizona, il a fait l'objet d'une RFC dans le cadre du groupe IPsec et est, avec ISAKMP et SKEME, à la base de l'échange de clef pour IPsec.

- Principe général:
  - Le but d'Oakley est de permettre le partage, de façon sûre entre les tiers, d'un ensemble d'informations relatives au chiffrement
  - En plus de D-H, Oakley possède plusieurs modes pour la génération des clefs.
  - Les trois composants du protocole sont :
    - Echange de cookies (éventuellement sans état),
    - Échange de valeurs publiques DIFFIE-HELLMAN (optionnel),
    - Authentification

Echange de clefs et authentification

La gestion des clés pour IPsec: ISAKMP & IKE

- ISAKMP est un protocole à objectif très général.
- Ces paramètres se réfèrent donc à une syntaxe déterminée par un nom de domaine d'interprétation (Domain of Interpretation).
- Le DOI finalisé qui nous intéresse est conçu pour satisfaire les besoins d'Internet (Internet Protocol Domain of Interpretation DOI1, RFC 2407).
  - Standards Security Architecture for the Internet Protocol (RFC 2401) et IKE (Internet Key Exchange RFC 2409).

Echange de clefs et authentification
ISAKMP

- ISAKMP est utilisable pour négocier, sous forme de SA, les paramètres relatifs à n'importe quel mécanisme de sécurité

- ISAKMP est prévu pour fonctionner indépendamment des mécanismes pour lesquels il travaille :
  - ISAKMP peut être implémenté directement au-dessus d'IP, ou au-dessus de tout protocole de la couche transport.
  - Port 500 sur UDP

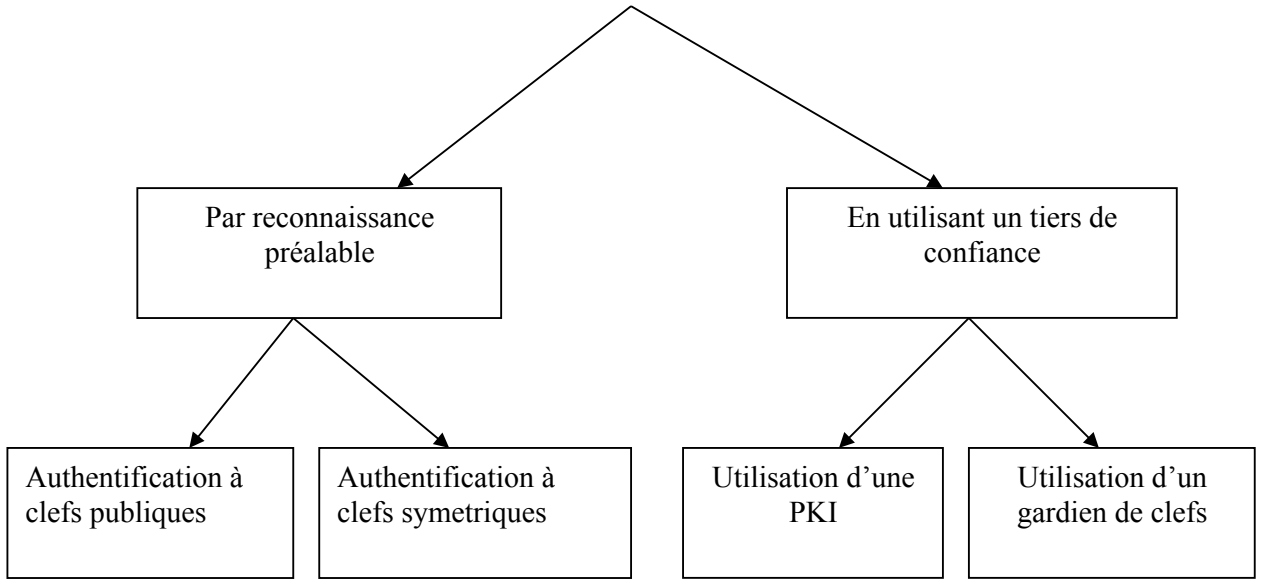
Echange de clefs et authentification
ISAKMP

- L'utilisation d'ISAKMP comporte deux phases :
  1. Etablissement d'une association primaire SA-ISAKMP pour le protocole ISAKMP lui-même et création d'une clé symétrique entre 2 machines.
  2. La seconde phase est réalisée quand 2 entités désirent communiquer en utilisant un protocole donné
     - Seuls les crypto-systèmes symétriques sont alors utilisés.
     - La durée de vie des associations secondaires peut être limitée en fonction du nombre de messages échangés.

- Une entité peut donc gérer de nombreuses SA

Echange de clefs et authentification
ISAKMP

- La première étape n'est que la seconde d'un processus complet.
- On trouve donc de nombreuses options de ISAKMP en fonction du mode d'authentification choisi :

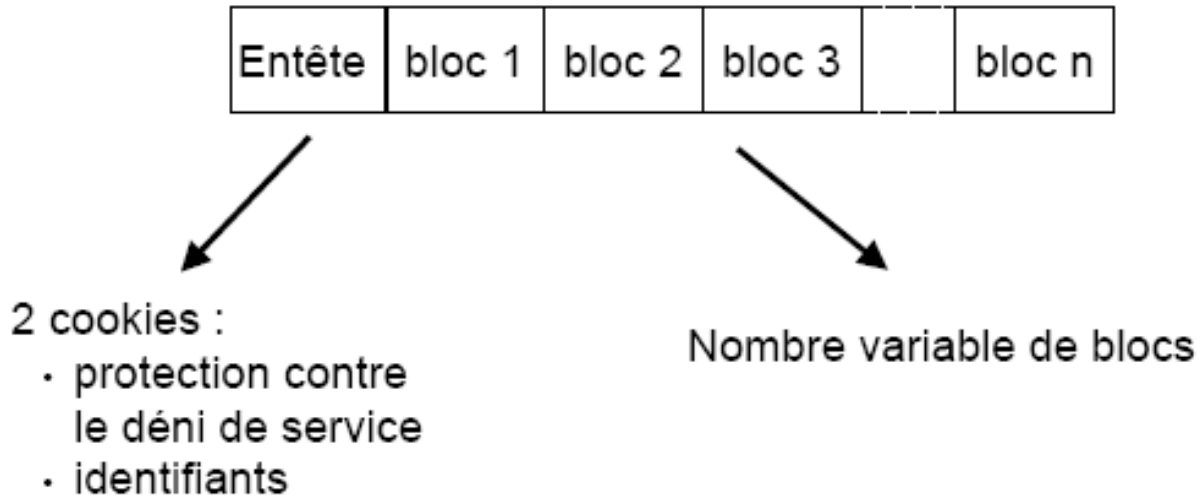


Echange de clefs et authentification
ISAKMP

- ISAKMP utilise une seule PDU qui contient une suite de champs chaînés (Payloads).
- ISAKMP est indépendant de la méthode de génération des clefs et des algorithmes de chiffrement et d'authentification utilisés.
- ISAKMP est une sorte de « kit de construction », puisque les messages d'ISAKMP sont constitués d'un en-tête suivi d'un nombre variable de blocs.

Echange de clefs et authentification
ISAKMP

- Les messages ISAKMP



Echange de clefs et authentification
ISAKMP

- Chaque message ISAKMP commence par un en-tête ISAKMP de longueur fixe.
  - Contrairement aux autres SA, elle n'est pas identifiée pas un SPI.
- Un champ Exchange Type permet de connaître le type d'échange en cours.
- L'en-tête ISAKMP comprend également un champ Next Payload qui indique le type du premier bloc du message.

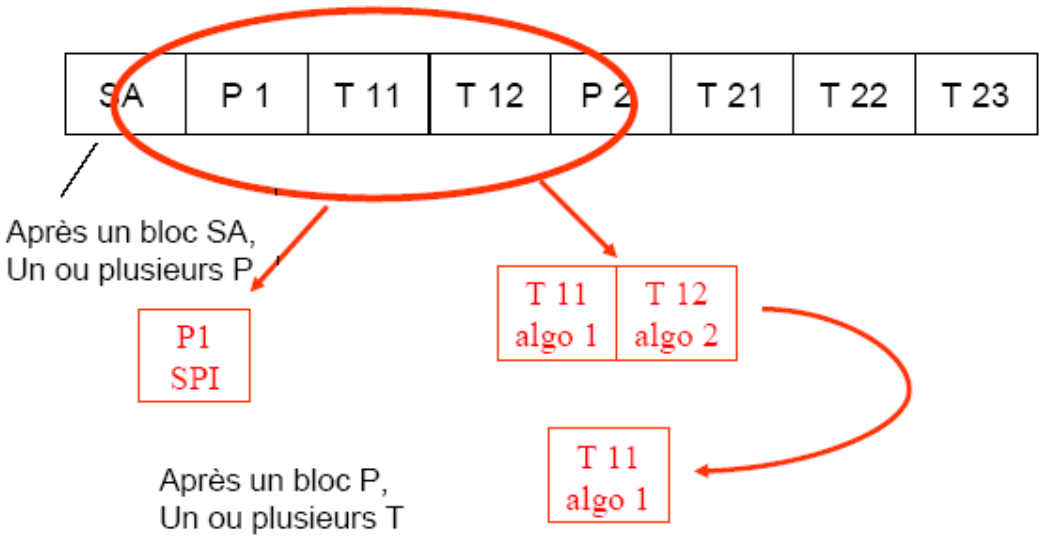
Echange de clefs et authentification
ISAKMP

- Il existe 13 types de blocs :

HDR	*ISAKMP Header*
SA	*Security Association*
P	*Proposal*
T	*Transform*
KE	*Key Exchange*
ID	*Identification*
CERT	*Certificate*
CR	*Certificate Request*
HASH	*Hash*
SIG	*Signature*
NONCE	*Nonce*
N	*Notification*
D	*Delete*
VID	*Vendor ID*

Echange de clefs et authentification
ISAKMP

- L'ensemble représenté pourrait être un ensemble de propositions envoyé par un tiers à un autre. Le destinataire de ce message doit répondre par une suite identique dans laquelle il ne conserve que la proposition ou le groupe de propositions retenue.



Echange de clefs et authentification
ISAKMP

- CERT (*Certificate*) : transport des certificats, ou toute information s'y rattachant. Un champ intitulé Certificate Encoding indique le type de certificat ou de donnée relative aux certificats contenus dans le champ Certificate Data.

- Les types définis actuellement sont :
  - PKCS #7 wrapped X509 certificate
  - PGP certificate
  - DNS signed key
  - X 509 certificate – (signature or key exchange)
  - Kerberos tokens
  - CRL, Authority revocation list ARL
  - SPKI certificate, X509 certificate

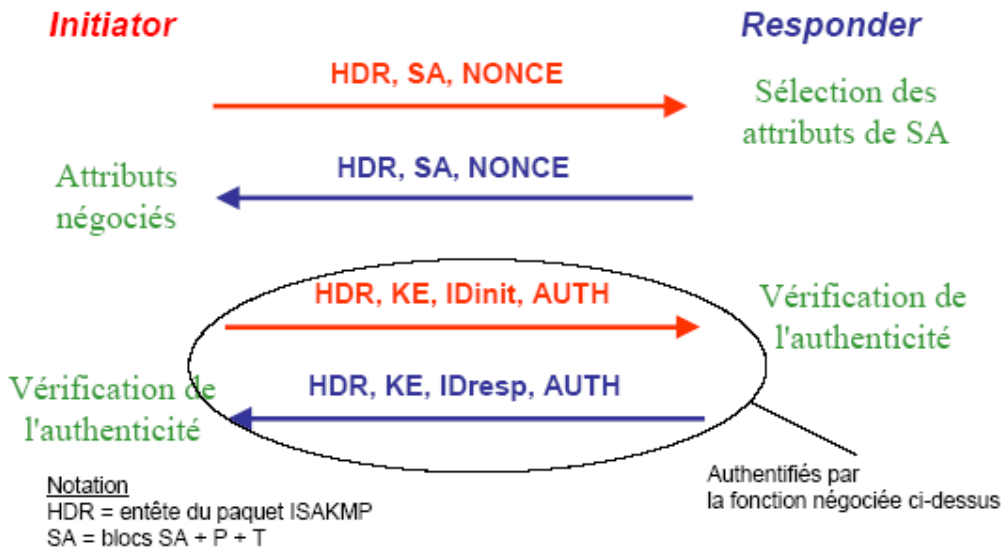
- CR (*Certificate Request*)

Echange de clefs et authentification
ISAKMP

- Les types d'échanges
  - A partir des blocs précédents, le protocole ISAKMP définit des types d'échanges (E*xchange Types*).
  - Il y a 5 types d'échanges par défaut :
    - Base Exchange (L'échange de base)
    - Identity Protection Exchange (L'échange de protection d'identité)
    - Authentication Only Exchange (L'échange d'authentification seule)
    - Aggressive Exchange (L'échange agressif)
    - Informational Exchange (L'échange d'information)
  - Ces échanges peuvent être utilisés durant la phase 1 ou 2.

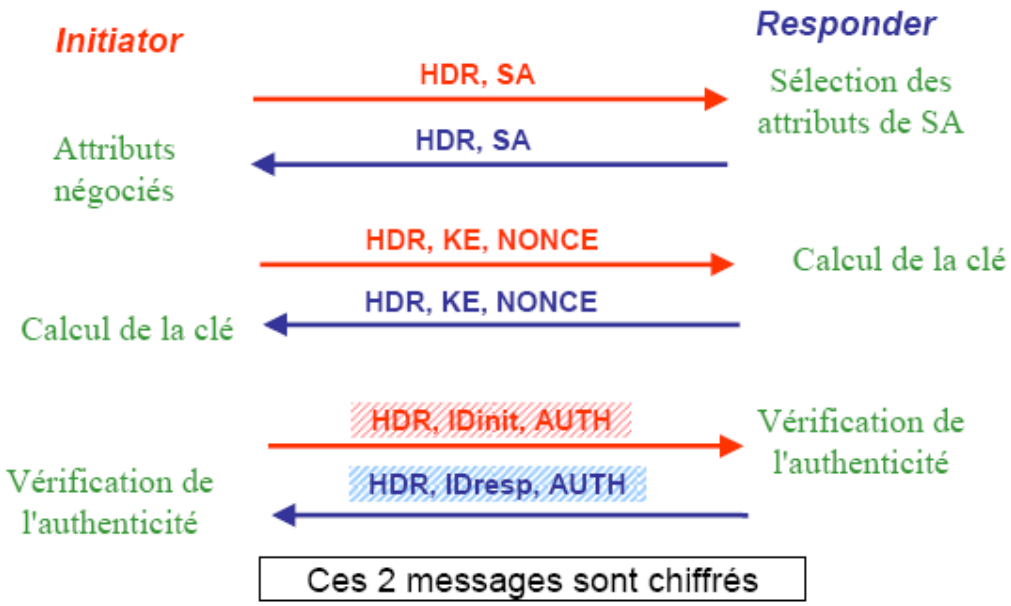
Echange de clefs et authentification
ISAKMP

- **Base Exchange** est conçu pour permettre le transfert simultané des données d'identification et des données servant à la génération de la clef



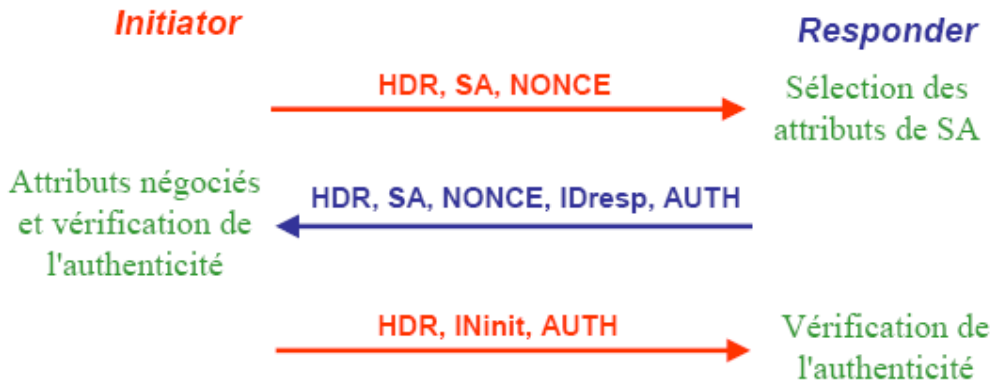
Echange de clefs et authentification
ISAKMP

- **Identity Protection Exchange** assure l'anonymat des tiers.



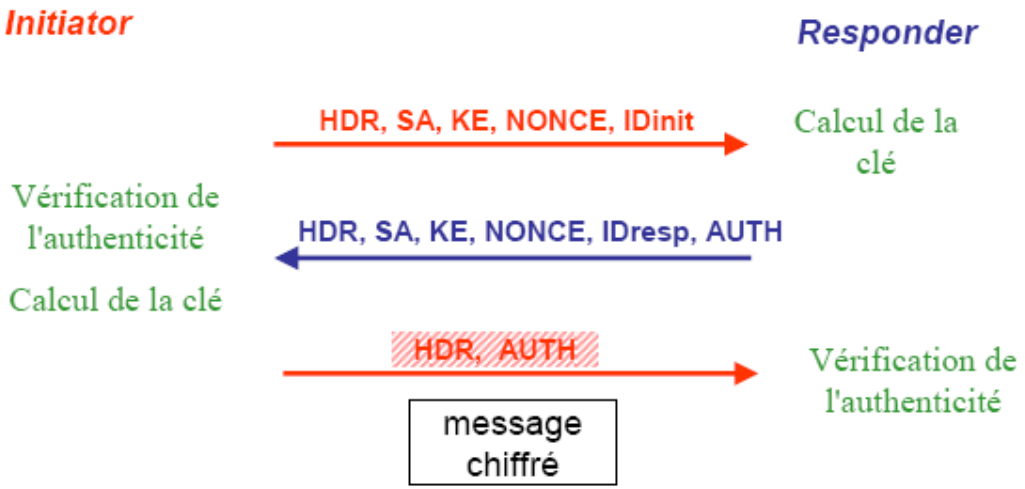
Echange de clefs et authentification
ISAKMP

- **Authentication Only Exchange** est conçu pour aboutir uniquement à l'authentification des tiers



Echange de clefs et authentification
ISAKMP

- **Aggressive Exchange** combine les données de négociation de la SA, d'authentification et d'échange de clef en un seul message



Echange de clefs et authentification
ISAKMP

- **Informational Exchange** est constitué d'un seul message et sert à transmettre une information relative à la gestion des SA : message d'erreur, information d'état, annonce de suppression de SA…

Echange de clefs et authentification
IPsec DOI

- Domaine d'interprétation pour IPSec
  - ISAKMP définit un cadre pour négocier les SA mais n'impose rien quant aux paramètres qui les composent.
  - Un document appelé « domaine d'interprétation » définit les paramètres négociés et les conventions relatives à l'utilisation de ISAKMP dans un cadre précis.
  - La RFC 2407 définit le DOI pour l'utilisation de ISAKMP pour IPsec.

Echange de clefs et authentification
IPsec DOI

- Bloc SA : situation
  - Utilisé dans le bloc SA de ISAKMP, le champ situation permet de préciser la situation à laquelle doit être rattachée la négociation.
  - Le DOI IPsec définit trois situations différentes:
    - Identity only
    - Secrecy
    - Integrity

- Bloc P : protocole de sécurité
  - ISAKMP, AH, ESP, IPCOMP

Echange de clefs et authentification
IPsec DOI

- Bloc T : transformation et attributs
  - Pour ISAKMP, cette méthode permet de choisir le protocole d'échange de clef à utiliser.
  - Pour AH : MD6, SHA-2, etc.
  - Pour ESP : AES, RC5, IDEA, CAST, BLOWFISH, 3IDEA, RC4, NULL, etc.

Echange de clefs et authentification
IPsec DOI

- Bloc ID
  - Le DOI IPsec ajoute au bloc ID les champs «Protocol ID» UDP, TCP… et «Port», et définit les modes d'identification suivants:
    - Adresse IPv4, adresse IPv6
    - Sous réseau IPv4 ou IPv6
    - Plage d'adresses IPv4 ou IPv6
    - FQDN foo.bar.com
    - User FQDN user@foo.bar.com
    - X500 Distinguished Name
    - KEY ID : information propre à un fournisseur et permettant d'identifier le secret partagé préalable à utiliser

Echange de clefs et authentification
IKE

- IKE - Internet Key Exchange : RFC 2409
- Le protocole de gestion des clefs associé à ISAKMP dans ce but est inspiré à la fois d'Oakley et de SKEME.
- D'autre part, IKE ne dépend pas d'un DOI particulier mais peut utiliser tout DOI.

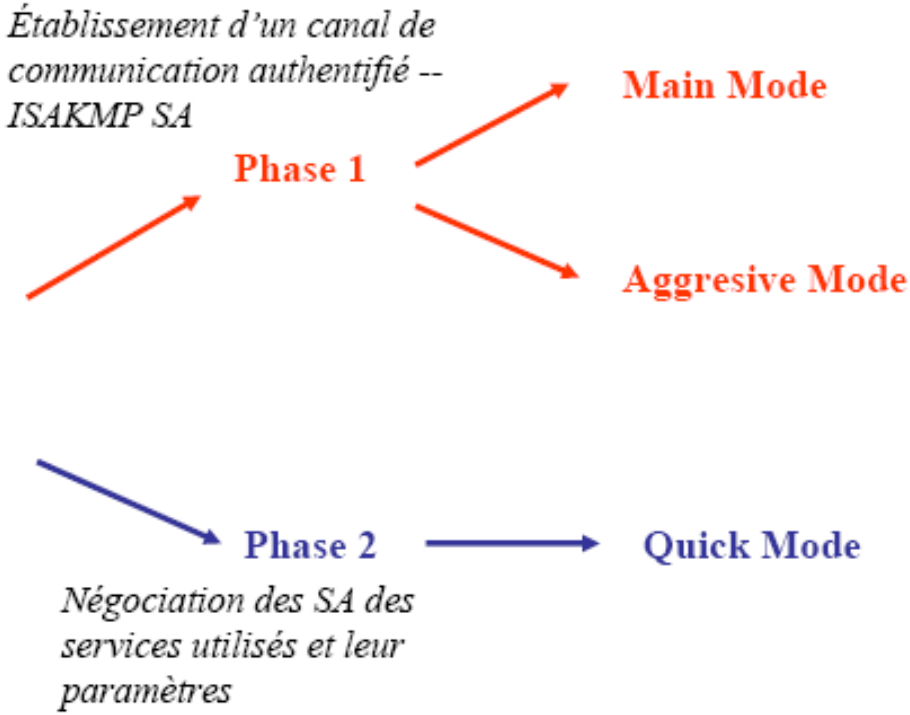
Echange de clefs et authentification
IKE

- IKE comprend 4 modes :
  - principal (Main Mode)
  - agressif (Aggressive Mode)
  - rapide (Quick Mode)
  - nouveau groupe (New Group Mode)

- **Main Mode** et **Aggressive Mode** sont utilisés durant la phase 1, **Quick Mode** est un échange de phase 2.

- **New Group Mode** sert à se mettre d'accord sur un nouveau groupe pour de futurs échanges DIFFIE-HELLMAN.

Echange de clefs et authentification
IKE

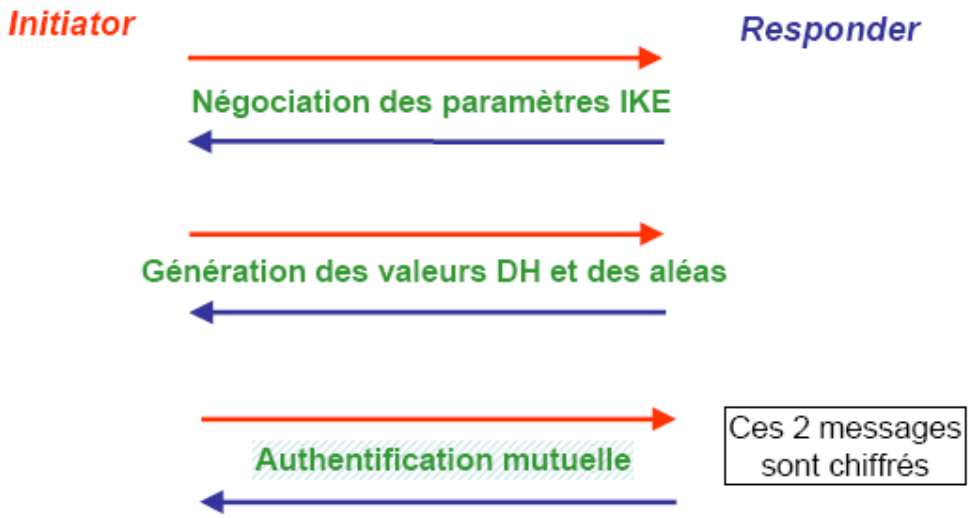


Echange de clefs et authentification
IKE

- Phase 1 : Main Mode est une instance de l'échange ISAKMP Identity Protection Exchange
  - Six messages sont générés par le mode Main Mode durant la phase 1 en vue d'établir :
    - **4 paramètres :**
    - un algorithme de chiffrement,
    - une fonction de hachage,
    - une méthode d'authentification
    - un groupe pour Diffie-Hellman
    - **3 clés :**
    - une pour le chiffrement,
    - une pour l'authentification
    - une pour la dérivation d'autres clés

Echange de clefs et authentification
IKE

- Phase 1 : Main Mode



Echange de clefs et authentification
IKE

- Phase 1 : Aggressive Mode
  - Aggressive Mode est une variante du mode Main Mode qui ne contient que 3 messages.

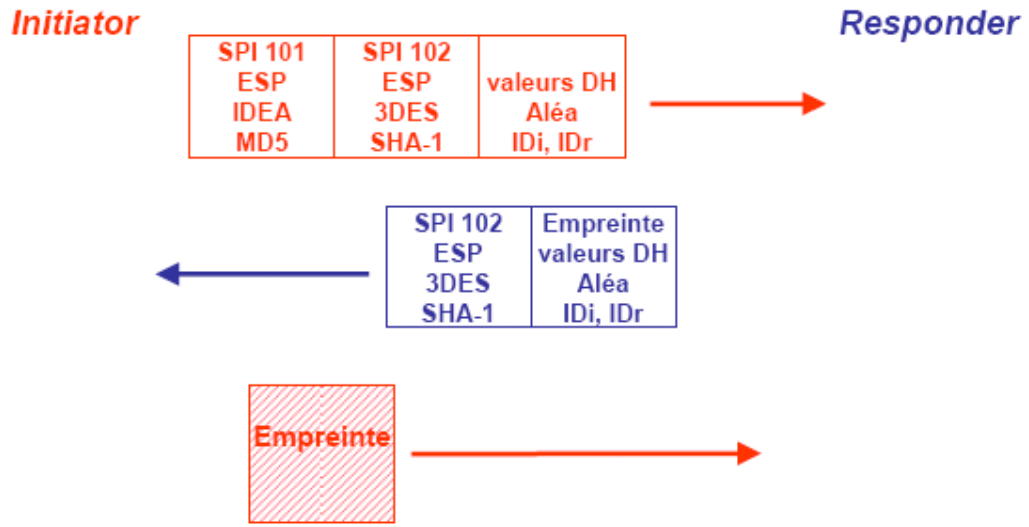
- Phase 2 : Quick Mode
  - Les messages échangés durant la phase 2 sont protégés en intégrité et en confidentialité grâce aux éléments négociés durant la phase 1.
  - Quick Mode est utilisé pour la négociation de SA pour des protocoles de sécurité donnés comme IPsec.

Echange de clefs et authentification
IKE

- Phase 2 : Quick Mode (suite)
  - Les échanges composant ce mode ont le rôle suivant:
    - Négocier un ensemble de paramètres IPsec (paquets de SA)
    - Echanger des nombres aléatoires, utilisés pour générer une nouvelle clef qui dérive de celle de la SA ISAKMP.

Echange de clefs et authentification
IKE

- Phase 2 : Quick Mode



- New Group Mode
  - Ce mode sert à négocier le groupe Diffie-Hellman si ce dernier n'a pas été établi durant le Main Mode.