INSA | INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

Aspects de sécurité et modèle OSI. IPsec.

Module Sécurité réseau

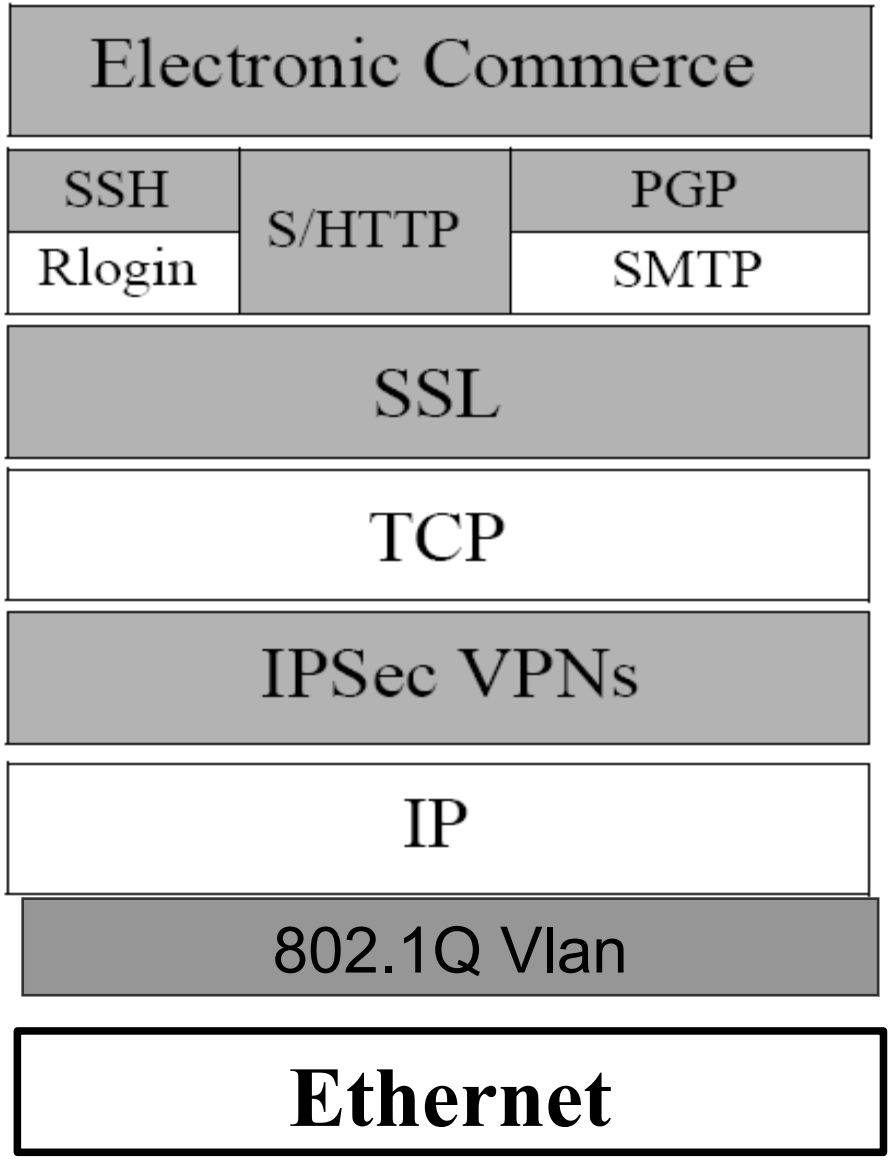
Promo 2022 STI 4A

M. Szpieg

Année 2020-2021

La sécurité dans les couches réseaux

Exemples de services de sécurité appliqués aux couches réseaux



Pourquoi IPSec ?

Les paquets IP (adresse + contenu) sont “faciles” à générer et difficiles à protéger et à authentifier.
Exemple socket de type « raw » sur Linux.

AH et ESP IPSec

Deux types de format de paquet IPSec sont utilisés.

Le mode AH ***Authentication Header :***

Ajouter un en-tête d'authentification cryptographique (*MAC-value*) afin d'obtenir

- Authentification de la source du paquet (adresse IP authentique) et de la destination
- Intégrité du contenu
- Non-Répudiation suivant l'algorithme cryptographique utilisé
- Non rejeu
- Donc attention le contenu de l'entête IP est impacté(PB NAT).

Le mode ESP ***(Encapsulating Security Payload) :***

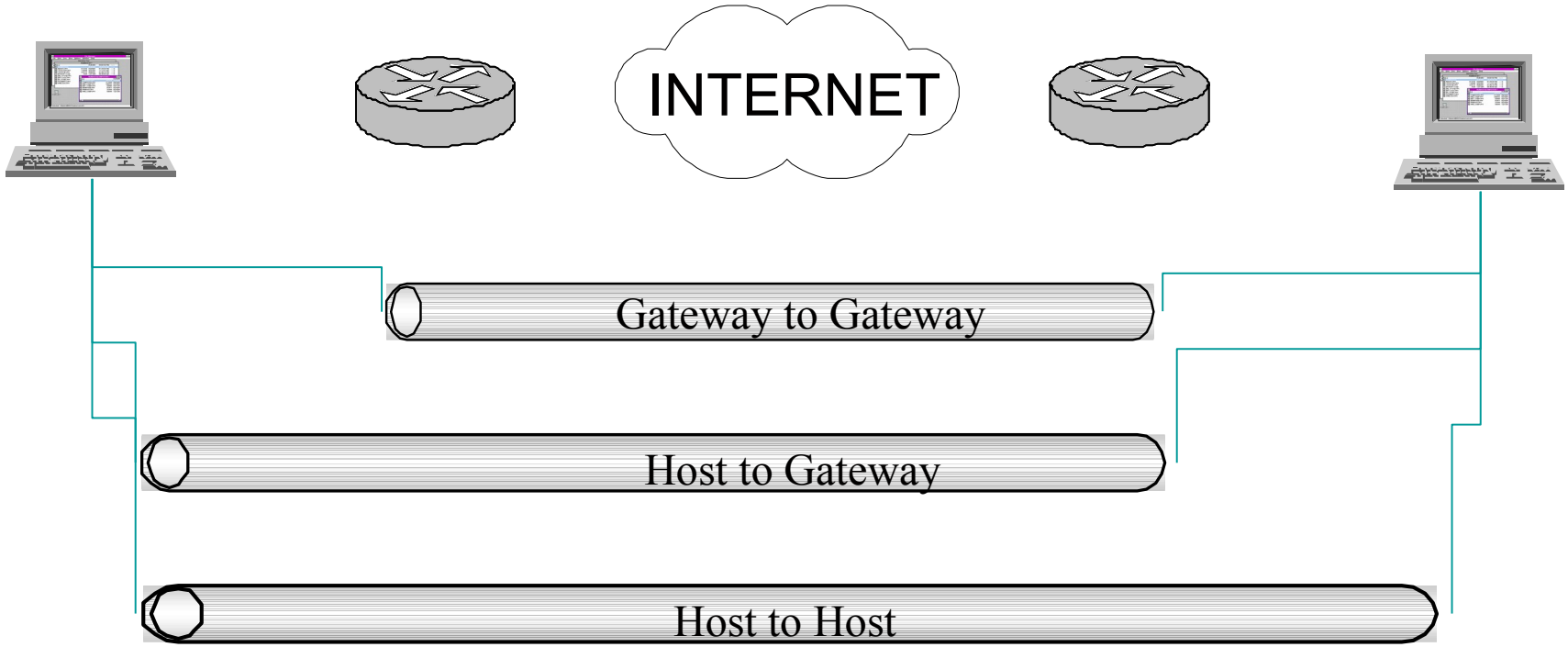
Encrypter le contenu des paquets IP afin d'obtenir, en plus :

- Confidentialité: Les paquets ne peuvent être lus que par le destinataire
- Ne concerne que le **payload** (charge utile) donc tout ce qui est au dessus de l'entête IP

Présentation IPSec

Le mode transport, traitement du paquet par IPSec de bout en bout ,seules les données se situant au dessus du protocole IP sont traitées par IPSec.

Le mode tunnel, traitement du paquet sur un chemin critique l'ensemble du paquet est traité par IPSec le datagramme ainsi traité est encapsulé dans un autre datagramme IP.



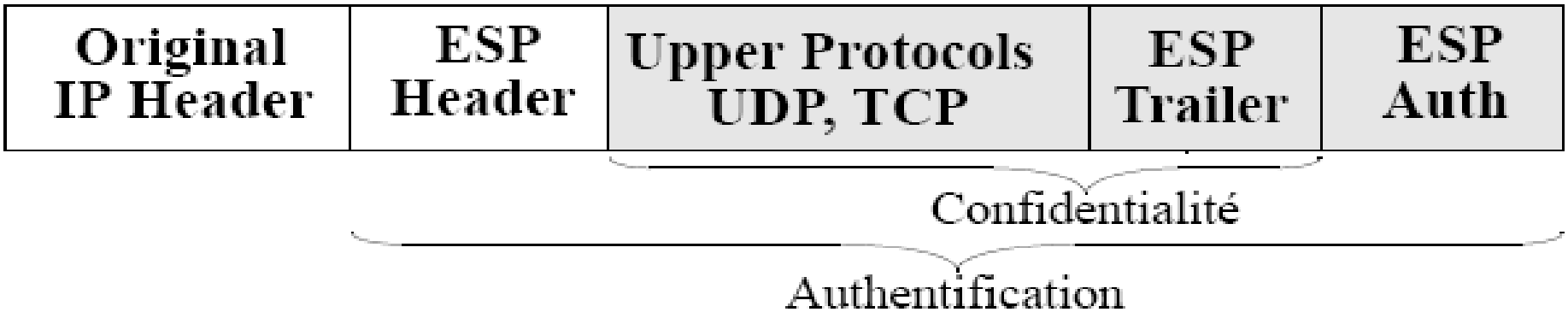
Présentation IPSec

Problème: Les paquets IP circulent en clair.

Solution: Encrypted Data (ESP *Encapsulating Security Payload*)

Paquet de la couche transport (UDP,TCP, etc.)

Ou paquet IP complet (tunnel mode)



Présentation IPSec

Un paquet contenant un ESP peut être traité par tous les intervenants d'un réseau IP mais ...

Les *ports* (UDP ou TCP) *source* et *destination* peuvent être cryptés, ceci pose des problèmes aux équipements de protection (*firewalls*...) qui se basent sur ces informations pour accepter ou refuser des paquets IP

La norme est indépendante de l'algorithme utilisé. Certains algorithmes possibles: DES,IDEA,RSA, etc.

ESP garantit l'authentification du paquet *encrypté*;

AH doit est utilisé pour assurer l'authentification du paquet *en clair*.

Les associations de sécurité

Les mécanismes utilisés par les en-têtes AH et ESP (chiffrage, signature,…) nécessitent que les deux éléments communiquant trouvent un accord sur la manière de communiquer (algorithmes,clefs utilisés,…)

Dans ce but IPSec s'appuie sur des entités appelées SA (Security Associations).

Une SA est donc une structure de données contenant les paramètres d'une connexion unidirectionnelle.

L'ensemble de ces SA actives est stocké dans une base de données appelée SAD (Security Association Database) ou parfois SADB

Une SA étant unidirectionnelle pour sécuriser une connexion dans les deux sens il est donc nécessaire d'avoir un couple de SA (une en sortie , l'autre en entrée). On peut pour certaines connexions utiliser plus d'un couple de SA, on utilise alors le terme de paquet de SA (bundle)

Contenu d'une SA

Une SA est composée de données qui l'identifient de manière unique :

- Adresse de destination
- Type IPSec utilisé AH ou ESP
- Un index du paramètre de sécurité SPI (Security Parameter Index)
  Bloc de 32 bits qui sera inscrit en clair dans l'en-tête de chaque paquet. La valeur de cet index sera donnée par le récepteur.

La SAD sera consultée à chaque paquet reçu ou à émettre.

Création d'une SA

Une SA peut être réglée de manière manuelle, néanmoins en règle général le processus suivi est plutôt dynamique.

La méthode manuelle ne permet pas de gérer l'expiration des clefs utilisées par la méthode dynamique.

Dynamiquement, IPSEC va générer des SA en utilisant un protocole de gestion des clefs appelé ISAKMP (Internet Security Association and Key Management Protocol) .

ISAKMP est développé par la NSA (National Security Agency)

Création d'une SA

En réalité ISAKMP est un cadre générique qui permet le choix entre plusieurs protocoles de clefs et qui peut être exploité par d'autres protocoles que IPSec (exemple TLS).
De ce fait des informations indiquant comment le protocole client utilise les demandes de clefs doivent être indiquées dans une base appelée DOI (Domain Of Interprétation)

A l'heure actuelle ISAKMP exploite deux protocoles d'échange de clefs SKEME(libre) et Oakley(libre) le protocole hybride ainsi obtenu est appelé IKE.

La politique de sécurité

La mise en place d' IPSec nécessite de maintenir une base de données qui contiendra la politique de sécurité à adopter.

C'est à l'utilisateur ou à l'administrateur système de maintenir cette base nommée SPD (Security Policy Database).
Dans cette base on indique en fonction de la nature d'un paquet s'il doit être traité par une SA, s'il peut transiter sans protection particulière ou s'il faut le jeter.

Exemple de la relation SPD SAD

SPD

Source	Destination	Sens	Politique	Mode
172.20.1.4	172.20.2.1	out	ESP	Transport
172.20.1.4	172.20.2.1	out	ESP	Transport

Source	Destination	Port	SPI	key	Politique
172.20.1.4	172.20.2.1	1000	50	« … »	3DES-CBC
172.20.1.4	172.20.2.1	any	51	« … »	DES-CBC

SAD

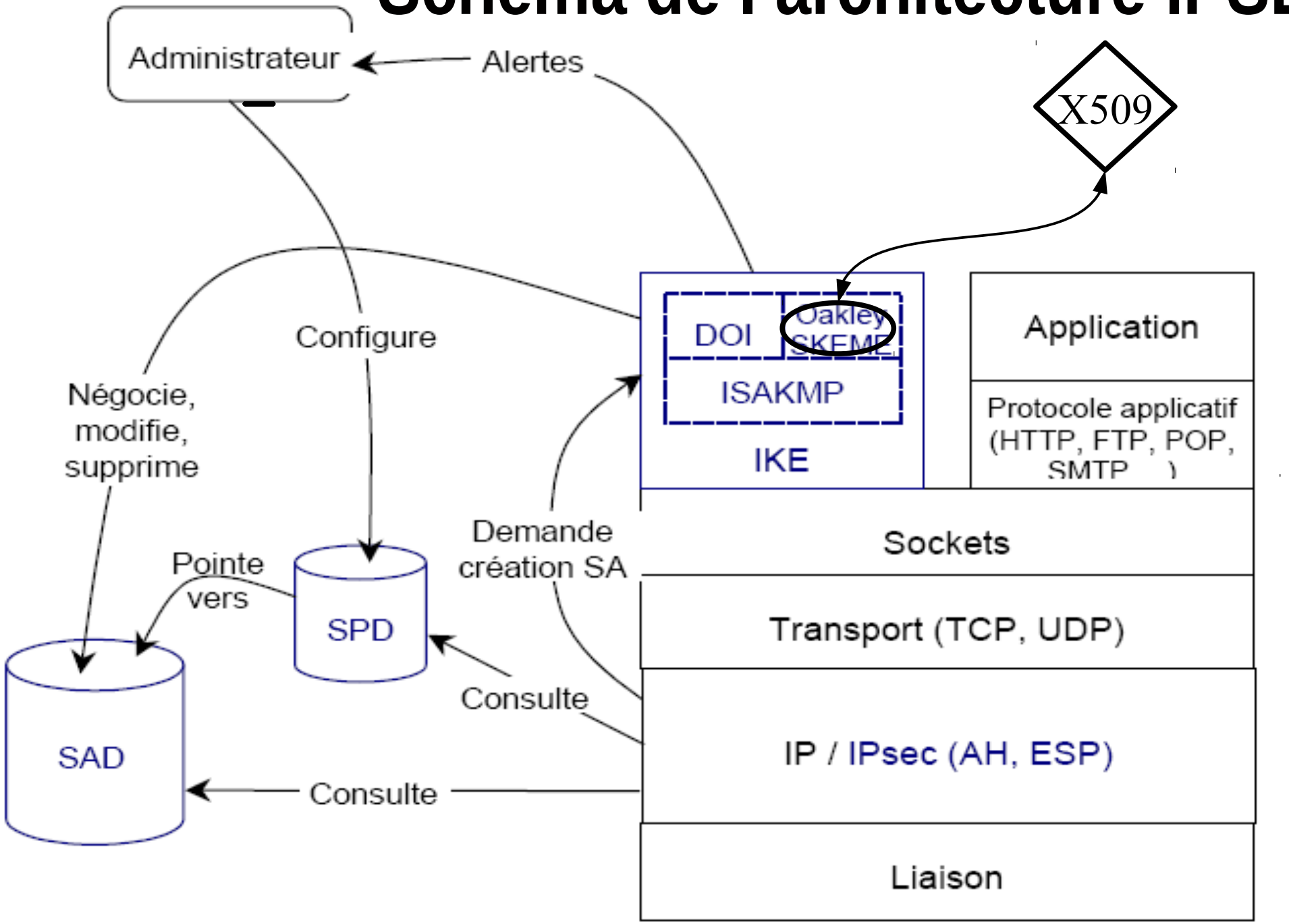
Exemple SPD

```
root@vmbourges-virtual-machine:/home/vm-bourges# setkey -DP
192.168.37.135[any] 192.168.37.134[any] 255
        fwd prio def ipsec
        esp/transport//require
        created: Nov 17 13:25:44 2020  lastused:
        lifetime: 0(s) validtime: 0(s)
        spid=66 seq=1 pid=3215
        refcnt=1
192.168.37.135[any] 192.168.37.134[any] 255
        in prio def ipsec
        esp/transport//require
        created: Nov 17 13:25:44 2020  lastused:
        lifetime: 0(s) validtime: 0(s)
        spid=56 seq=2 pid=3215
        refcnt=1
192.168.37.134[any] 192.168.37.135[any] 255
        out prio def ipsec
        esp/transport//require
        created: Nov 17 13:25:44 2020  lastused:
        lifetime: 0(s) validtime: 0(s)
        spid=49 seq=0 pid=3215
        refcnt=1
```

Exemple SAD

```
root@vmbourges-virtual-machine:/home/vm-bourges# setkey -D
192.168.37.135 192.168.37.134
        esp mode=transport spi=1(0x00000001) reqid=0(0x00000000)
        E: des-cbc  31323334 35363738
        A: hmac-md5  31323334 35363738 39303132 33343536
        seq=0x00000000 replay=0 flags=0x00000000 state=mature
        created: Nov 17 13:25:44 2020   current: Nov 17 13:26:41 2020
        diff: 57(s)     hard: 0(s)      soft: 0(s)
        last:                           hard: 0(s)      soft: 0(s)
        current: 0(bytes)       hard: 0(bytes)  soft: 0(bytes)
        allocated: 0    hard: 0 soft: 0
        sadb_seq=1 pid=3204 refcnt=0
192.168.37.134 192.168.37.135
        esp mode=transport spi=1(0x00000001) reqid=0(0x00000000)
        E: des-cbc  31323334 35363738
        A: hmac-md5  31323334 35363738 39303132 33343536
        seq=0x00000000 replay=0 flags=0x00000000 state=mature
        created: Nov 17 13:25:44 2020   current: Nov 17 13:26:41 2020
        diff: 57(s)     hard: 0(s)      soft: 0(s)
        last:                           hard: 0(s)      soft: 0(s)
        current: 0(bytes)       hard: 0(bytes)  soft: 0(bytes)
        allocated: 0    hard: 0 soft: 0
        sadb_seq=0 pid=3204 refcnt=0
```

Schéma de l'architecture IPSEC



En-tête AH

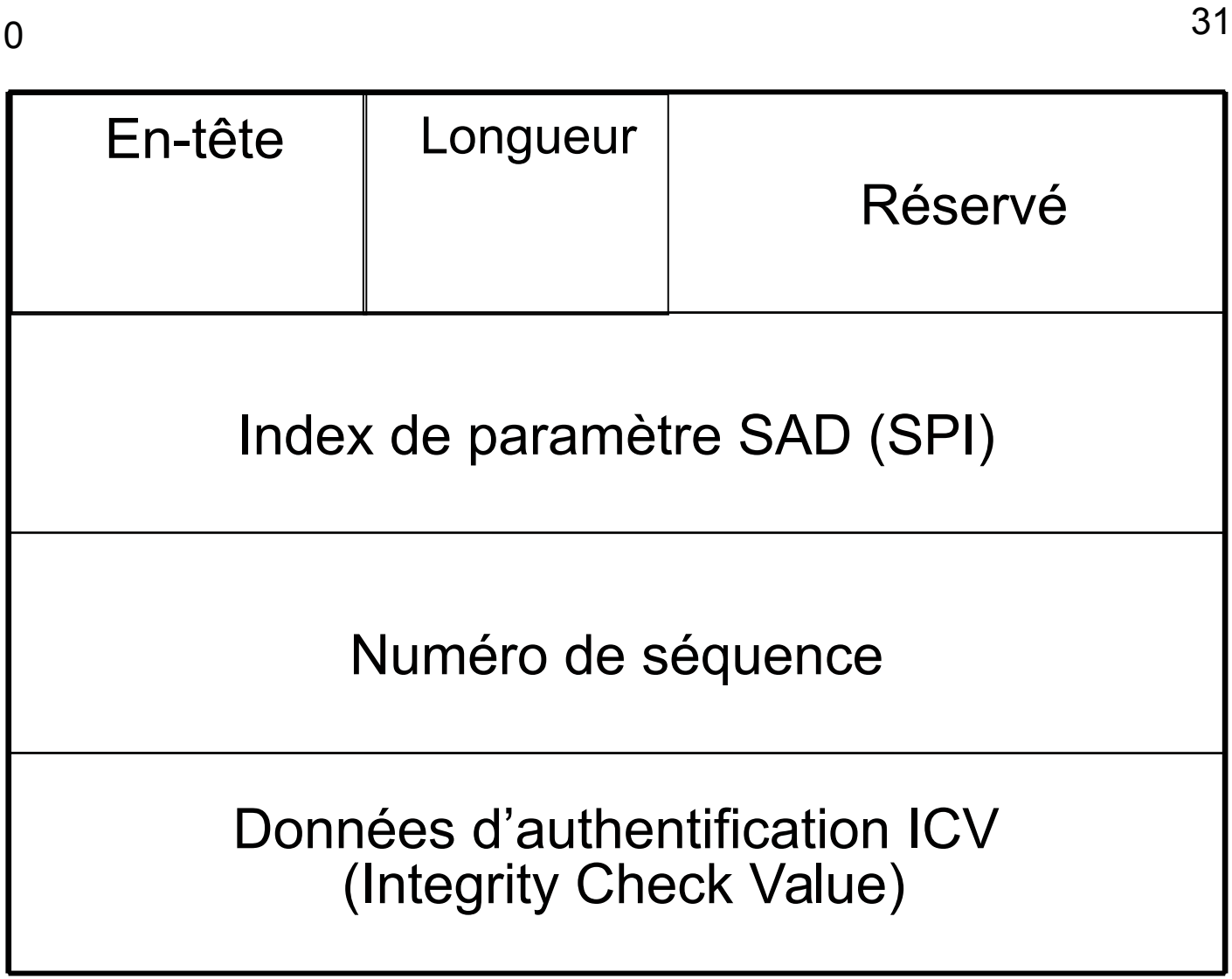
Il garantit :

- L’authentification ;
- l‘intégrité ;
- L’anti-rejeu ; parfois la non répudiation.

Il ne garantit pas

- La confidentialité.

En-tête AH


0
31
En-tête
Longueur
Réservé
Index de paramètre SAD (SPI)
Numéro de séquence
Données d'authentification ICV
(Integrity Check Value)

En-tête AH

Les différents champs :

En-tête suivant : Indique le protocole qui suit l'en-tête AH. En mode transport TCP ou UDP en mode tunnel IPV4 ou IPV6.

Longueur des données utiles : en mots de 32 bits –2.

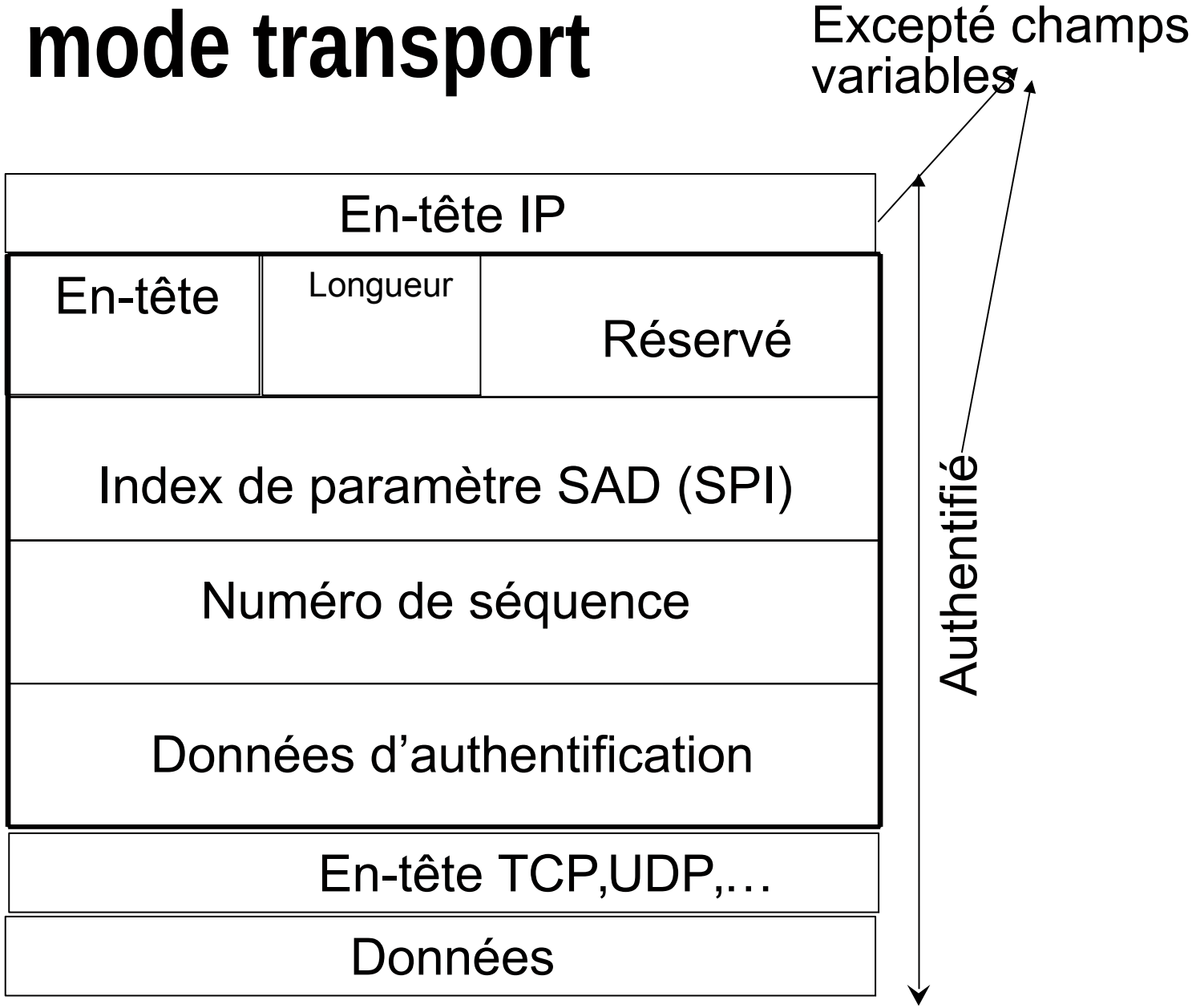
Réservé : inutilisé doit être à 0.

SPI : Index du paramètre de sécurité.

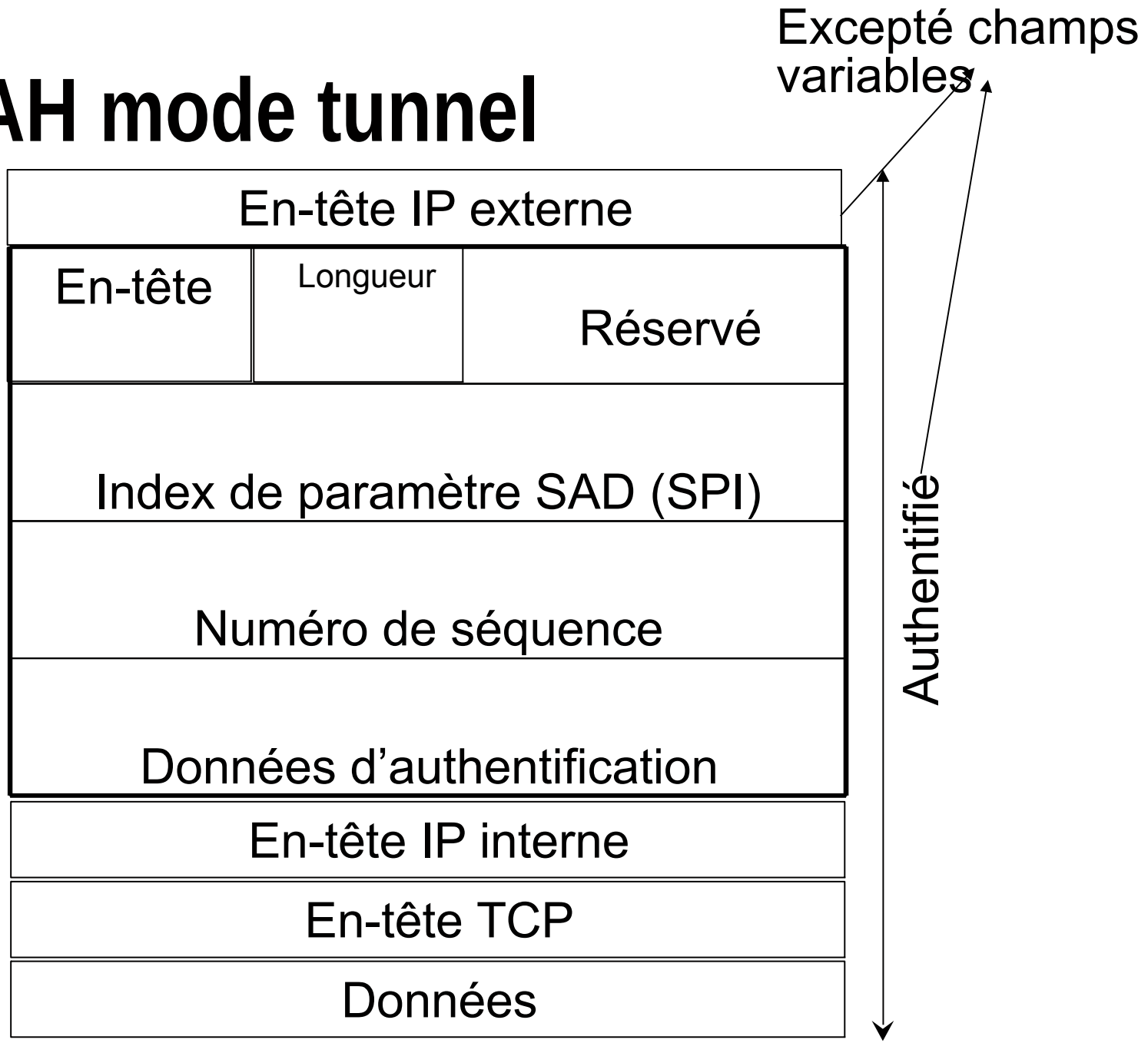
Numéro de séquence : Numéro unique croissant inséré par l'expéditeur évitant le rejeu.

Données d'authentification : contient le résultat de la fonction d'intégrité.
ICV : *Integrity Check Value*

AH mode transport



AH mode tunnel

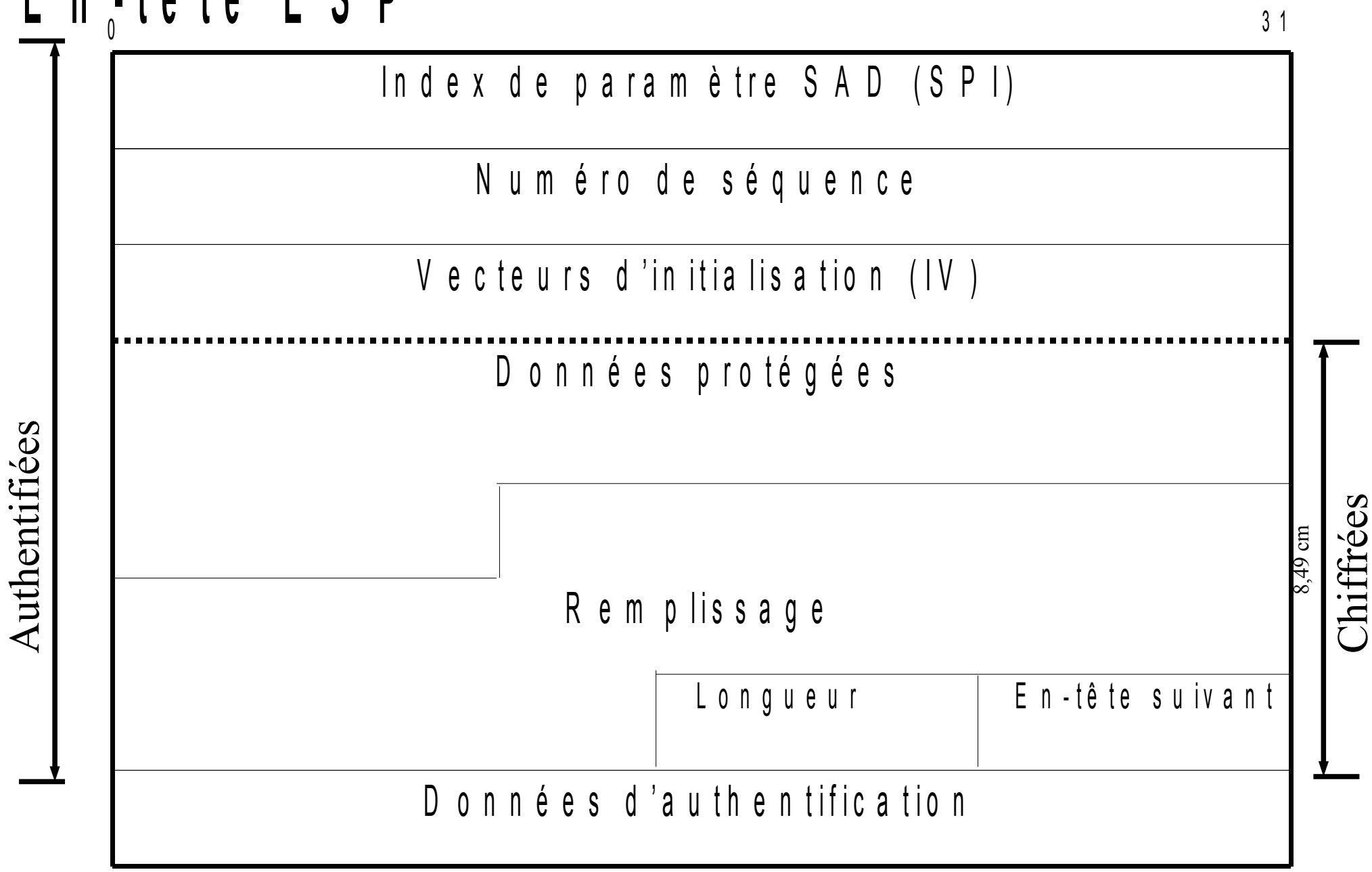


En-tête ESP

Rappel il garantit :

- La confidentialité ;
- L'authentification ; **Du payload**
- L'intégrité ; **Du payload**
- L'anti-rejeu ;
- Et parfois la non répudiation.

En-tête ESP


0
31
Index de paramètre SAD (SPI)
Numéro de séquence
Vecteurs d'initialisation (IV)
Données protégées
Remplissage
Longueur
En-tête suivant
Données d'authentification
Authentifiées
Chiffrées
8,49 cm

En-tête ESP

Les différents champs :

SPI : sélectionné au moment de l'échange IKE par le destinataire. Champ authentifié mais pas crypté.

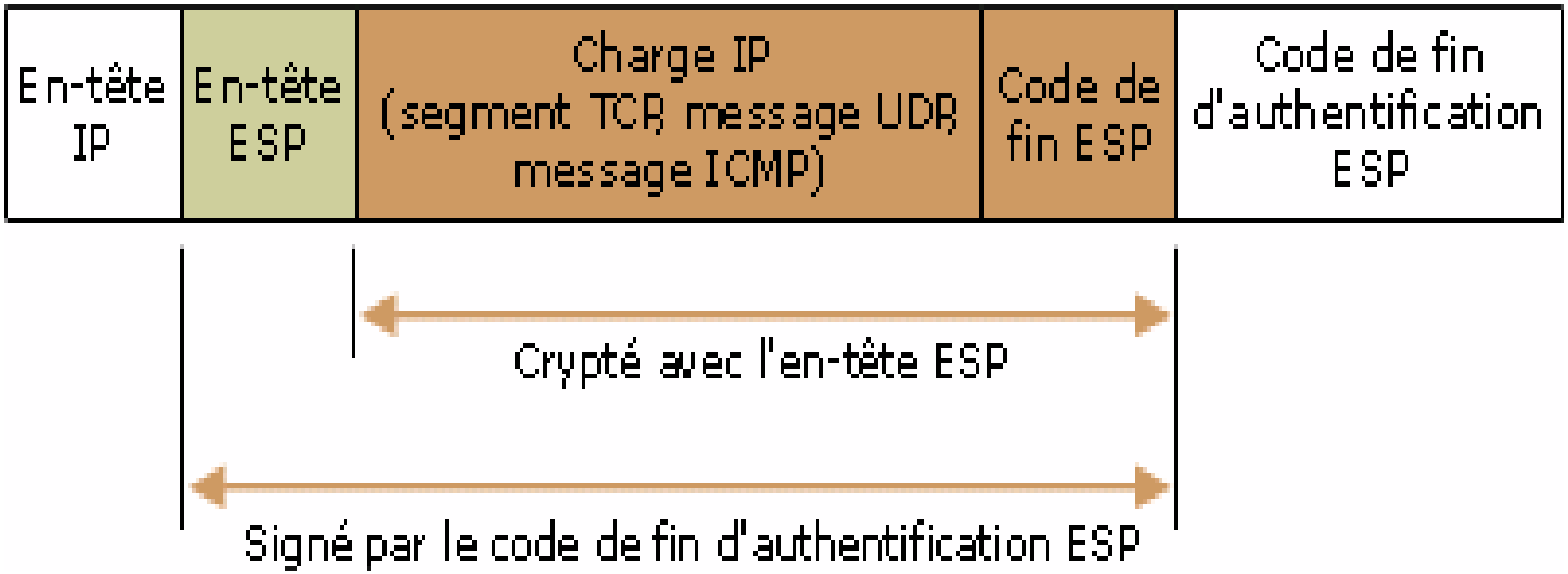
Numéro de séquence : Numéro unique croissant inséré par l'expéditeur évitant le rejeu. Authentifié mais pas crypté.

IV : vecteur d'initialisation pouvant être utilisé par un algorithme. 8 octets.Authentifié mais pas chiffré

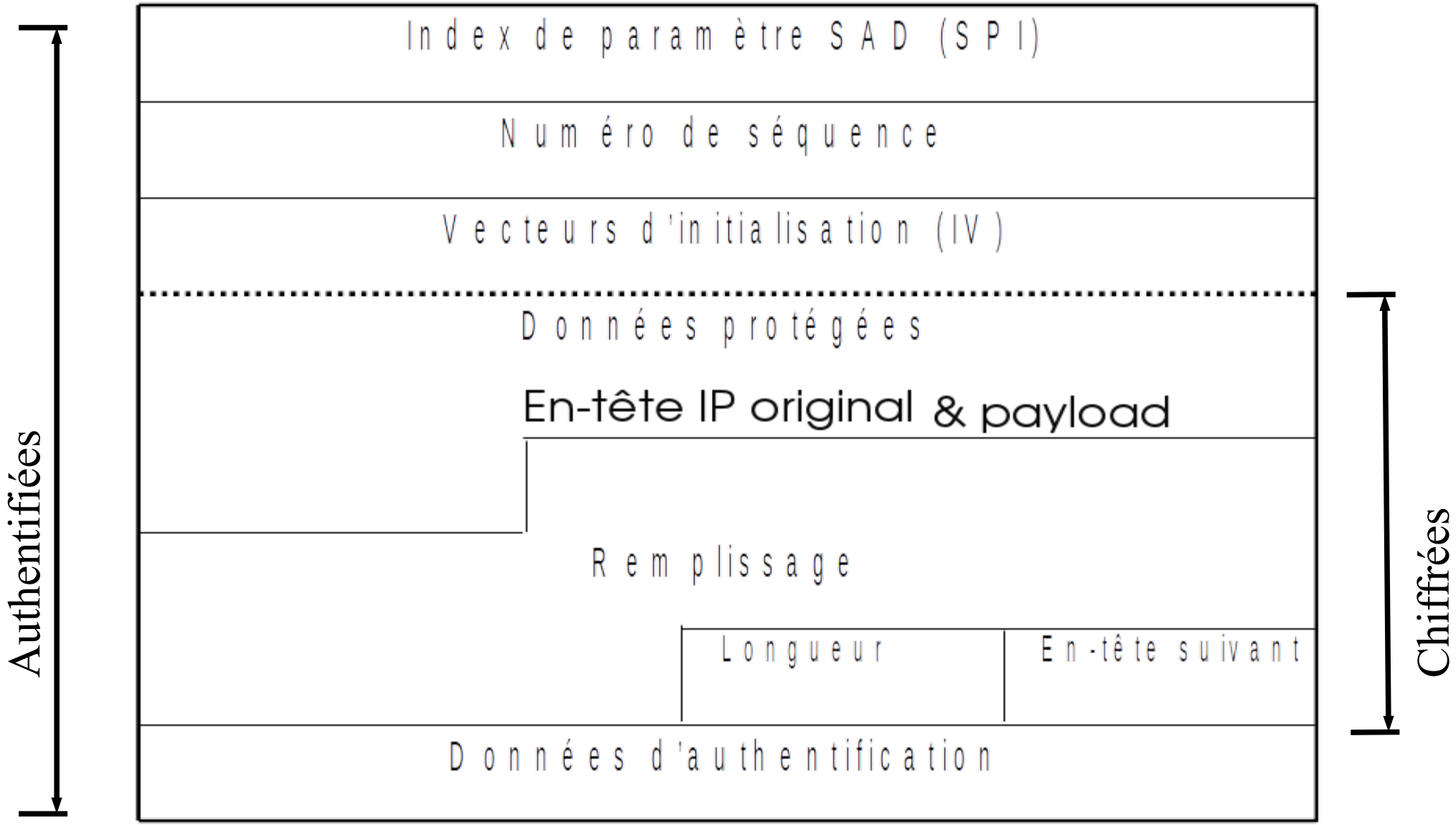
Données protégées : authentifiées et chiffrées

Remplissage : permet l'alignement pour certains algorithmes qui utilisent le chiffrement par blocs de longueur fixe permet aussi de masquer la longueur réelle. Authentifié et chiffré.

Insertion en-tête ESP mode transport



En-tête ESP mode tunnel



Exemple de lignes de configuration

```
## Flush the SAD and SPD
#
flush;
spdflush;
spdadd 192.168.190.128 192.168.190.129 any -P out ipsec esp/transport//require;
add 192.168.190.128 192.168.190.129 esp 1 -E des-cbc "12345678" -A hmac-md5 "1234567890123456";
spdadd 192.168.190.129 192.168.190.128 any -P in ipsec esp/transport//require;
add 192.168.190.129 192.168.190.128  esp 1 -E des-cbc "12345678" -A hmac-md5 "1234567890123456";
```