DE LA RECHERCHE À L'INDUSTRIE

Master 2 SeCReTS
Concepts Sécurité et Réseaux

IPSec

www.cea.fr

23 novembre 2015

A quoi ça sert ?

IPSec : *Internet Protocol Security*

- Protéger et/ou authentifier des communications sur des réseaux IP
- Protocole de niveau 3
- Développé initialement pour IPv6
- Norme indépendante de l'algorithme utilisé
- *RFC {4301,4302,4303}*

Cas d'utilisation

- S'assurer de la confidentialité de tout protocole basé sur IP
- Faire communiquer deux sous réseaux au travers d'un lien supposé non sûr

AH et ESP

IPSec est basé sur 2 protocoles pour la sécurisation des flux : *AH* et *ESP*

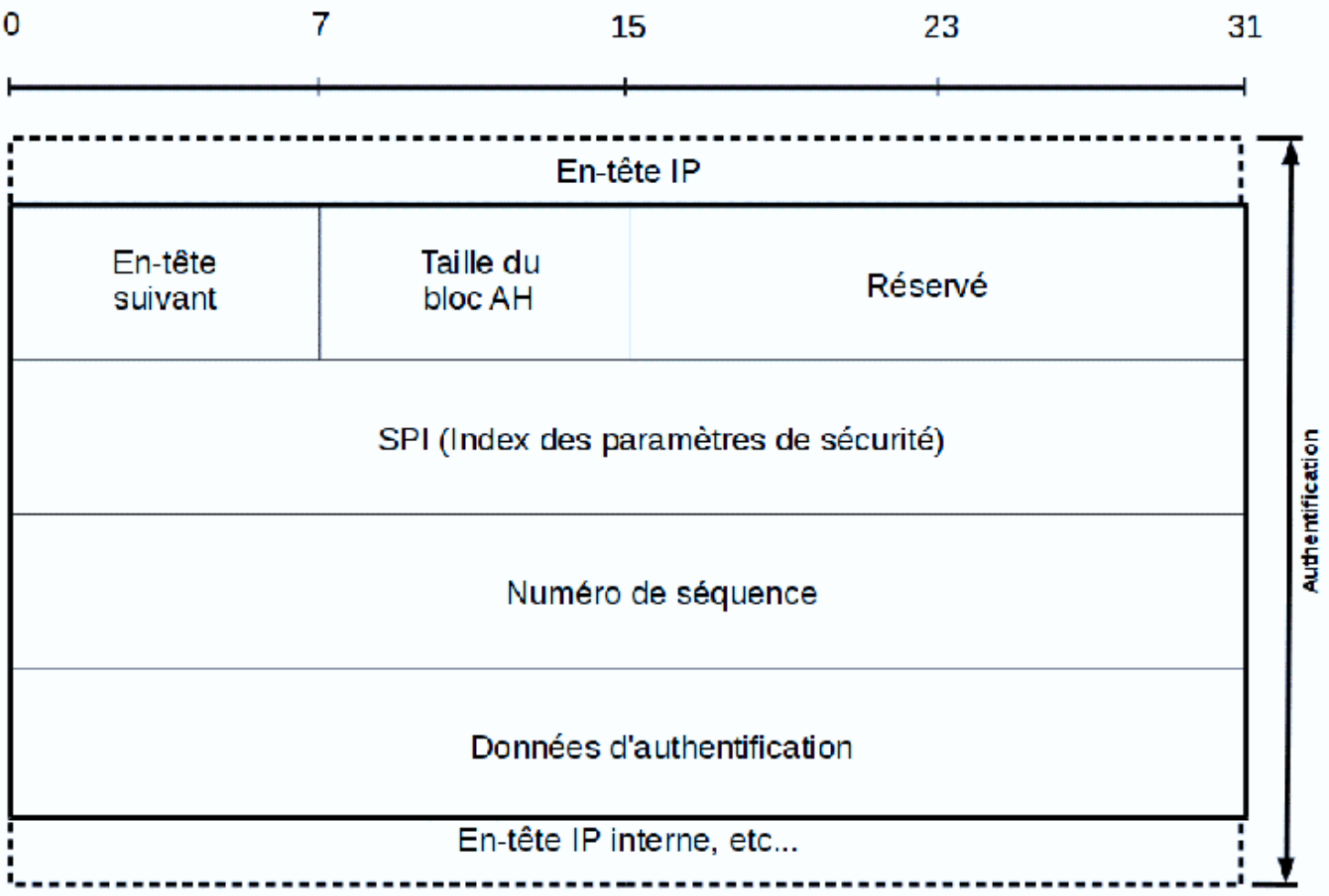
AH : Authentication Header

- Authentification de la source du paquet (authentification de l'en-tête IP)
- Intégrité du contenu
- Non rejeu.

En-tête AH

- En-tête suivant (TCP, UDP, IP)
- Longueur des donnes utiles
- Réservé : inutilisé doit être a 0
- SPI : index
- Numéro de séquence
- Données d'authentification, résultat de la fonction de hashage (ICV pour *Integrity Check Value*)

En-tête AH


0
7
15
23
31
En-tête IP
En-tête suivant
Taille du bloc AH
Réservé
SPI (Index des paramètres de sécurité)
Numéro de séquence
Données d'authentification
En-tête IP interne, etc...
Authentification

AH et ESP

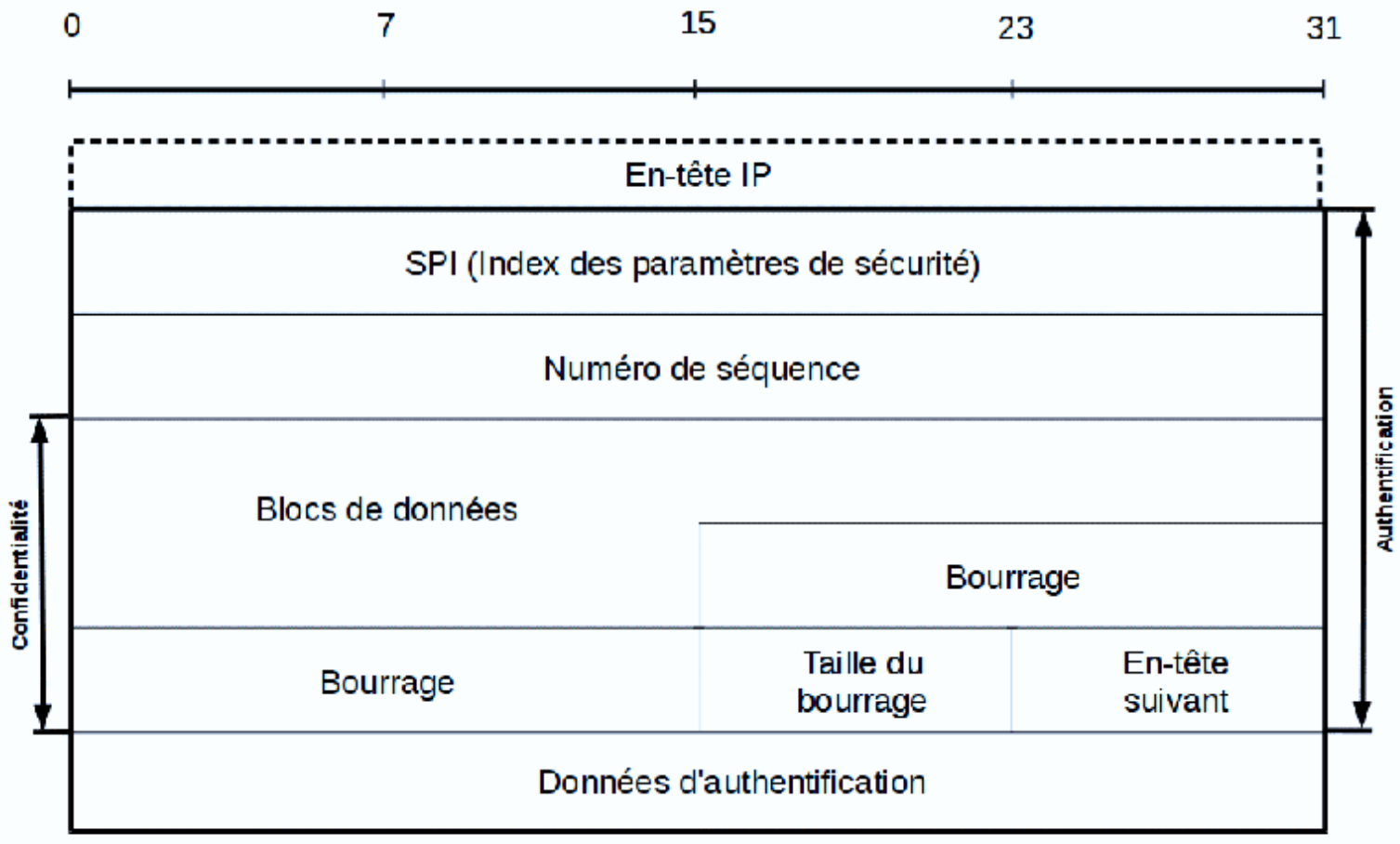
ESP : Encapsulating Security Payload

- Chiffrer le contenu des paquets IP afin d'avoir en plus la confidentialité : les paquets ne peuvent être lus que par le destinataire.
- Impossible pour des équipements intermédiaires de faire du filtrage par port.

En-tête ESP

- SPI : index en clair, authentifié mais pas crypté
- Numéro de séquence : authentifié mais pas crypté
- IV : vecteur d'initialisation pouvant être utilisé par l'algorithme : 8 octets authentifiés mais pas cryptés
- Données protégées : authentifiés et cryptés
- Remplissage : Authentifié et crypté
- Longueur de remplissage : permet au destinataire de retirer les octets de remplissage
- En tête suivant : indique le protocole qui suit l'en-tête ESP
- Données d'authentification : contient le résultat d'une fonction de hashage si demandé

En-tête ESP


0
7
15
23
31
En-tête IP
SPI (Index des paramètres de sécurité)
Numéro de séquence
Blocs de données
Bourrage
Bourrage
Taille du bourrage
En-tête suivant
Données d'authentification
Confidentialité
Authentification

Les différents modes de fonctionnement

Chacun des protocoles AH et ESP peut être implémenté de 2 manières :

Transport

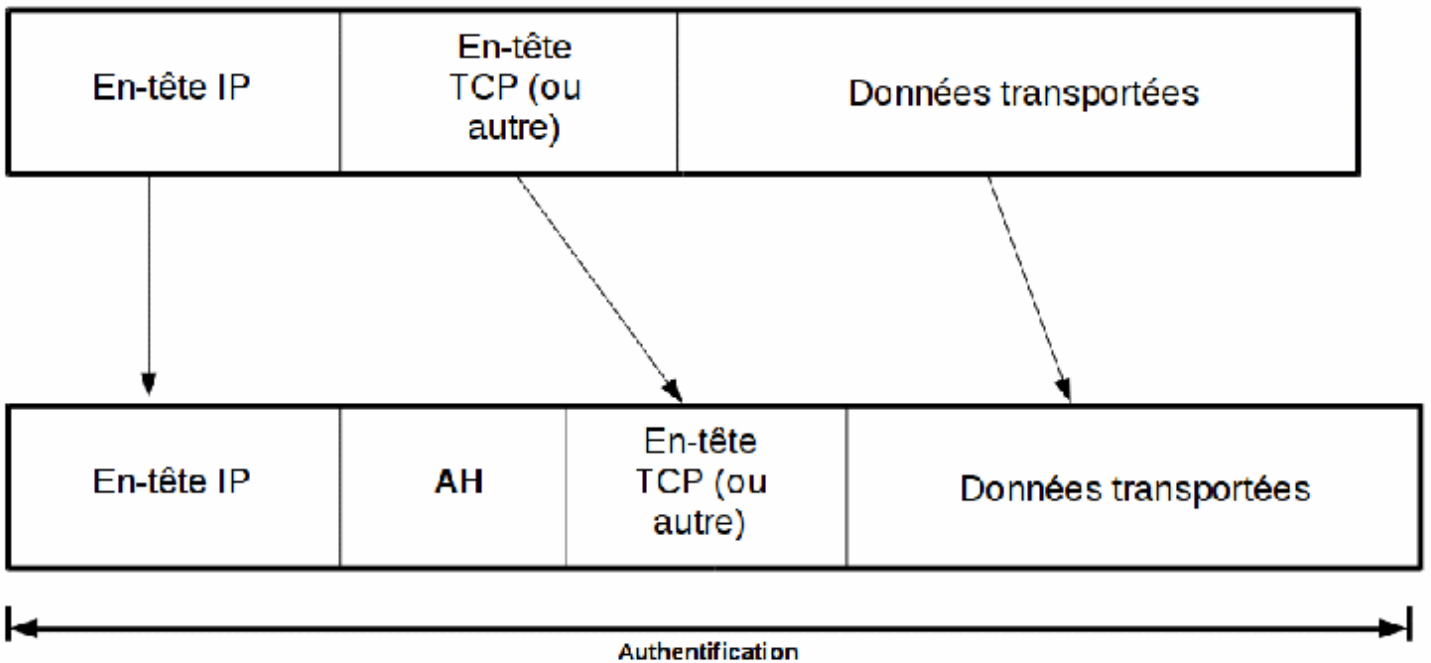
- On encapsule tout ce qui est au dessus de IP
- Le routage des paquets n'est pas modifié
- Utilisé pour les communications *Host-to-Host*

Tunnel

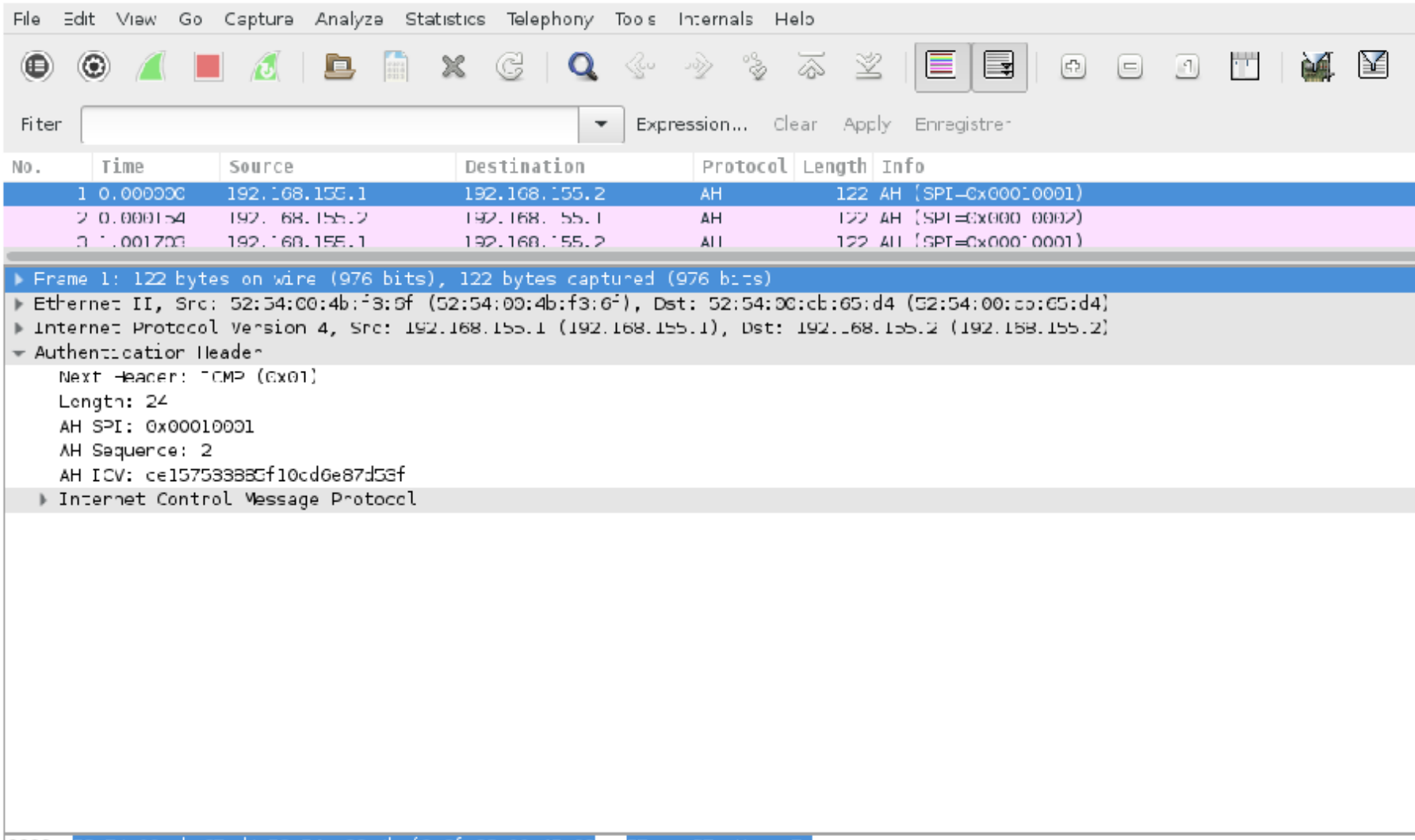
- On encapsule le paquet IP complet dans un nouveau paquet IP
- Utilisé pour les communications *Site-to-Site* et *Host-to-Site*

Exemples avec le protocole AH

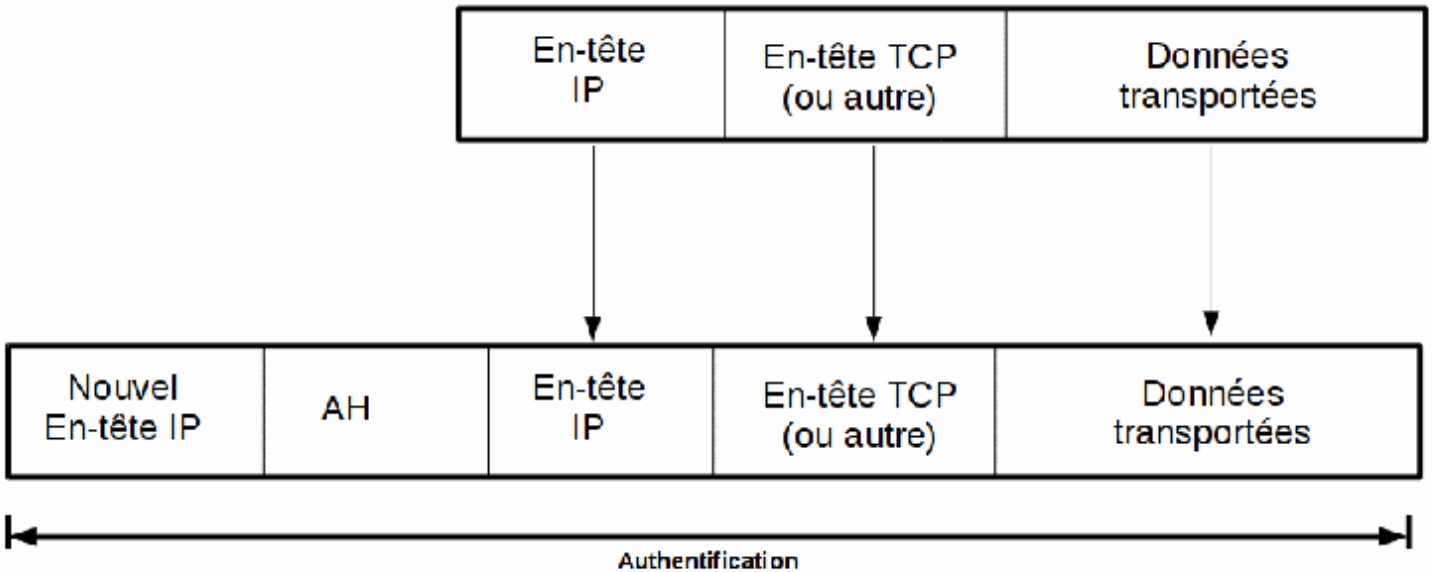
AH en mode transport



AH en mode transport

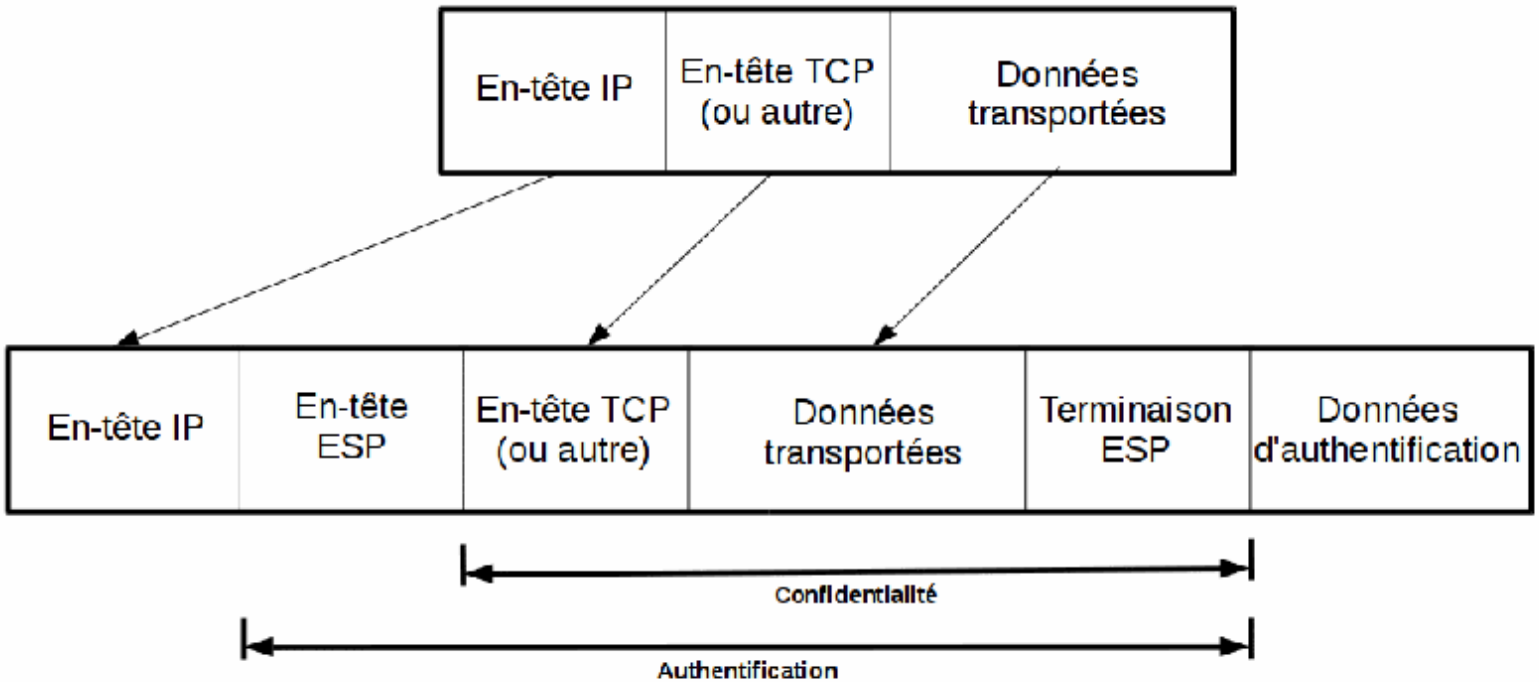


AH en mode tunnel

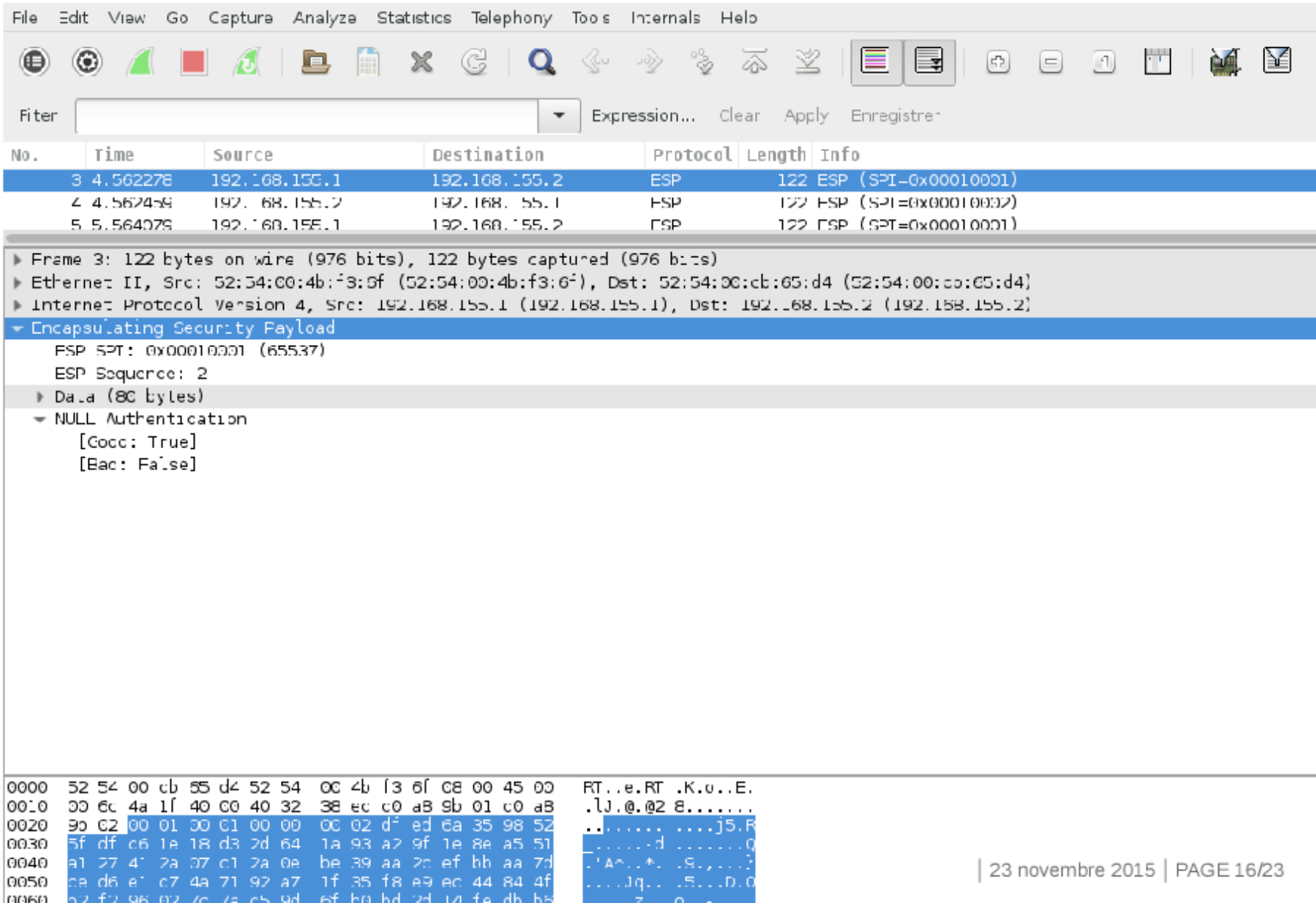


Exemples avec le protocole ESP

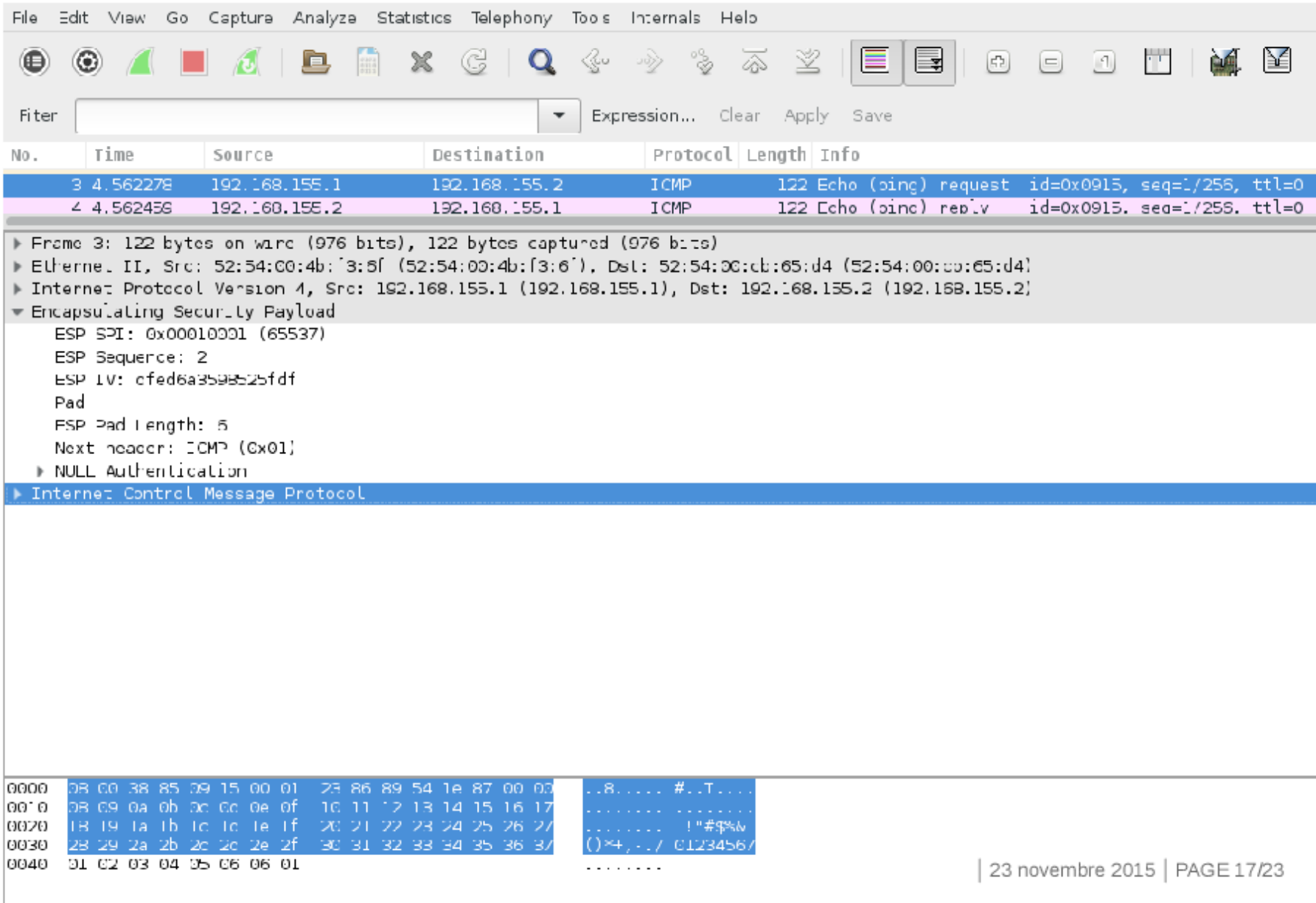
ESP en mode transport



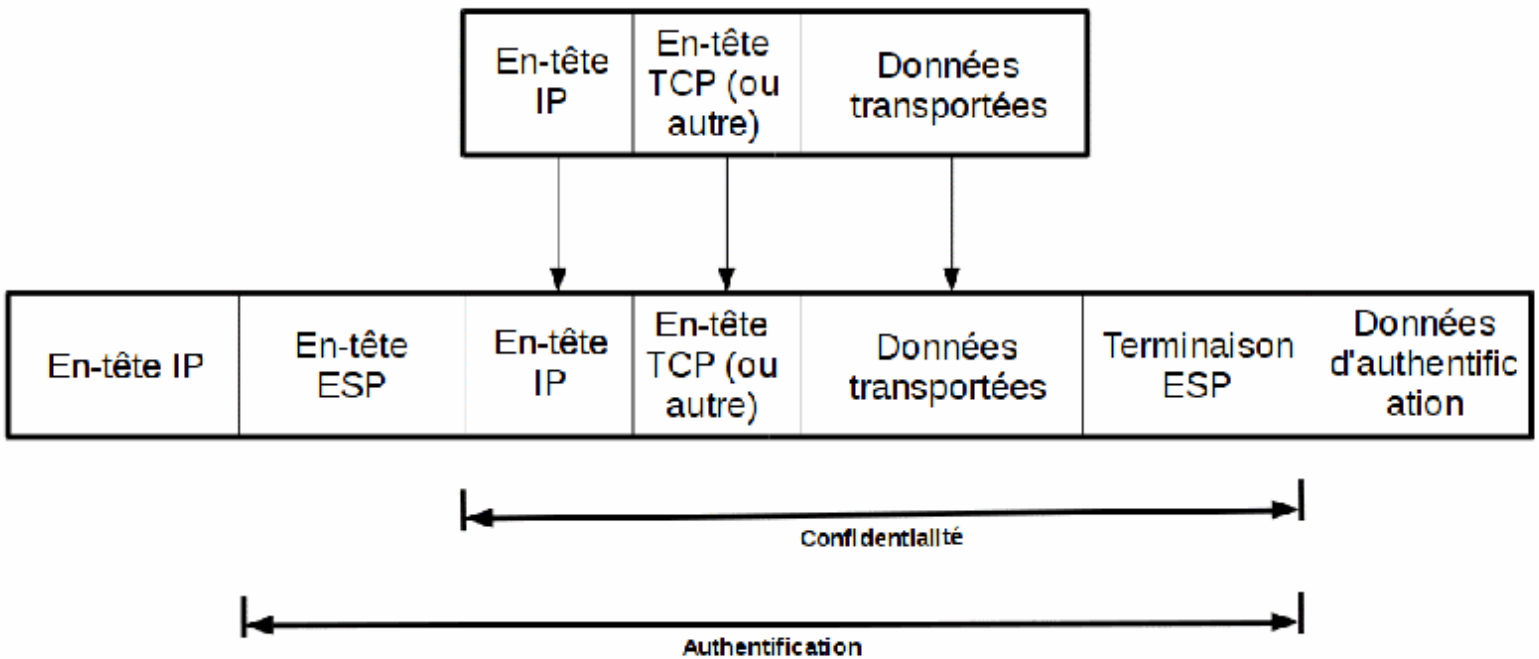
ESP en mode transport



ESP en mode transport



ESP en mode tunnel



Politique de sécurité, SPD

Security Policy Database

IPSec nécessite de maintenir une base de données qui contiendra la politique de sécurité à adopter.

- Cette base s'appelle la SPD
- Elle indique si un paquet doit être traité par une SA, transmit en clair ou rejeté
- Celle-ci est consulté quel que soit le trafic

Exemple d'ajout d'une entrée à la SPD :

```
spdadd 192.168.1.1 192.168.1.2 icmp \
  -P out ipsec esp/transport//require;
```

SA : Security Associations

Security Associations

IPSec s'appuie sur des entités appelées SA

- Structure de données contenant les paramètres d'une connexion UNIDIRECTIONNELLE
- Un couple de SA est nécessaire pour sécuriser une connexion
- L'ensemble des SA actives est stocké dans une base de données appelée SAD (Security Association Database)

Exemple de paramétrage d'une SA :

```
add 192.168.1.1 192.168.1.2 esp 0x1001 -m transport \
  -E des-cbc "12345678" -A hmac-md5 "1234567890123456";
```

SA : *Security Associations*

Une SA est composée notamment de :

- Adresses IP source et destination
- Mode de fonctionnement IPSec : AH ou ESP
- Un index SPI (Security Parameter Index) : valeur de 32 bits
- Compteur de numéro de séquence (paquets émis)
- Paramètres AH/ESP

La SAD est consulté pour chaque paquet reçu ou à émettre

SPD vs SAD

- **La SPD nous dicte ce que l'on doit faire**
- **La SAD nous dit comment le faire**

Échange de clefs

Les deux extrémités doivent se mettre au préalable d'accord sur la façon de communiquer (algorithme, clef,)

- De manière manuelle : ne permet pas de gérer le déploiement des clefs ni leur expiration
- Dynamiquement : on utilise pour cela un protocole d'échange de clefs (IKE, ISAKMP). Les clefs peuvent être renouvelées périodiquement.