

DE LA RECHERCHE À L'INDUSTRIE



www.cea.fr

Master 2 SeCReTS

Concepts Sécurité et Réseaux

IPSec

23 novembre 2015

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

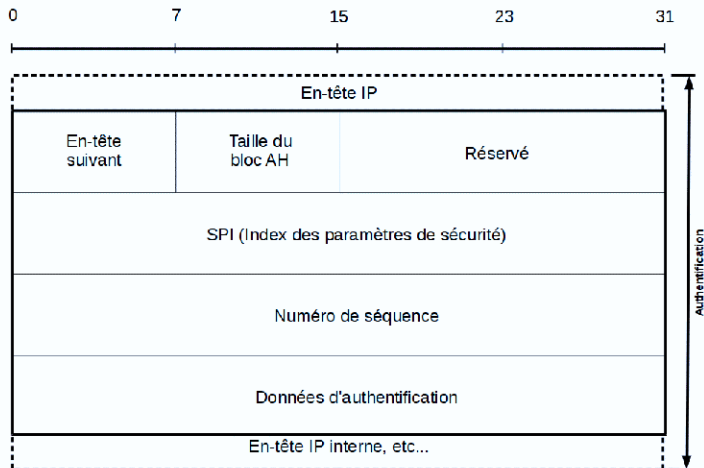
- S'assurer de la confidentialité de tout protocole basé sur IP
- Faire communiquer deux sous réseaux au travers d'un lien supposé non sûr

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.

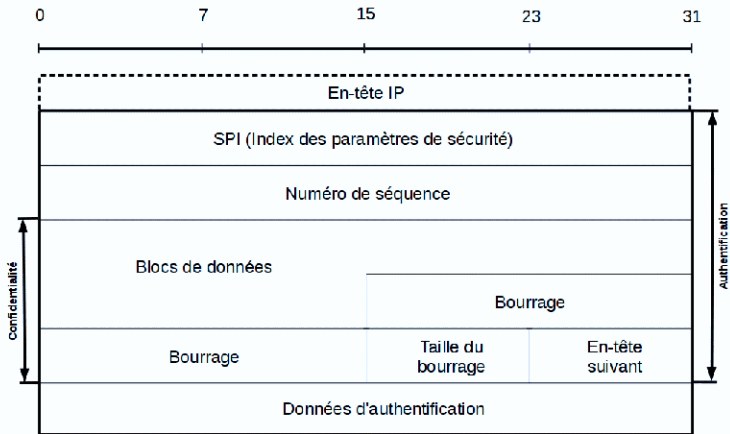
- En-tête suivant (TCP, UDP, IP)
- Longueur des données utiles
- Réserve : inutilisé doit être à 0
- SPI : index
- Numéro de séquence
- Données d'authentification, résultat de la fonction de hachage (ICV pour *Integrity Check Value*)



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.

- 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



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

Transport

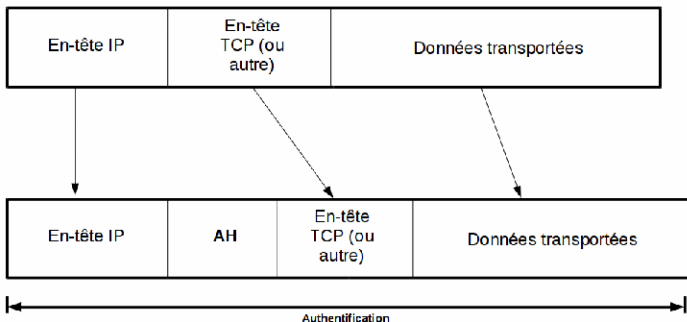
- On encapsule tout ce qui est au dessus de IP
- Le routage des paquets n'est pas modifié
- Utilisé pour les communications *Host-to-Host*

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



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter Expression... Clear Apply Enregistrer

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.155.1	192.168.155.2	AH	122	AH (SPI=0x00010001)
2	0.000124	192.168.155.2	192.168.155.1	AH	122	AH (SPI=0x00010002)
3	0.001700	192.168.155.1	192.168.155.2	AH	122	AH (SPI=0x00010001)

► Frame 1: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)

► Ethernet II, Src: 52:54:00:4b:f3:0f (52:54:00:4b:f3:0f), Dst: 52:54:00:c3:65:d4 (52:54:00:c3:65:d4)

► Internet Protocol Version 4, Src: 192.168.155.1 (192.168.155.1), Dst: 192.168.155.2 (192.168.155.2)

▼ Authentication Header

Next Header: ICMP (0x01)

Length: 24

AH SPI: 0x00010001

AH Sequence: 2

AH ICV: ce15753388cf10cd6e87d53f

► Internet Control Message Protocol

0000 52 54 00 c3 65 d4 52 54 00 4b f3 0f 08 00 45 00 RT...RT...K...E...

0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

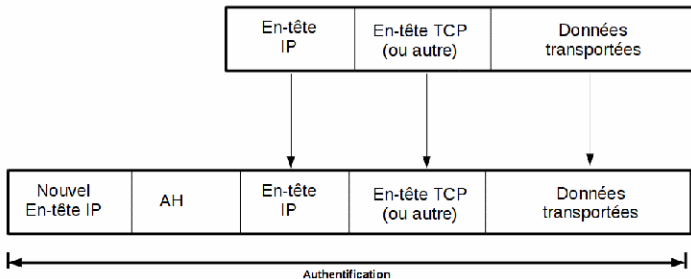
0030 75 33 88 5f 10 c3 6e 87 d5 3f 08 00 12 0d 09 25

0040 00 01 4b 87 89 54 1c ee 00 00 08 09 ca 0b 0c 0d ...K...T... ..

0050 0a cf 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d

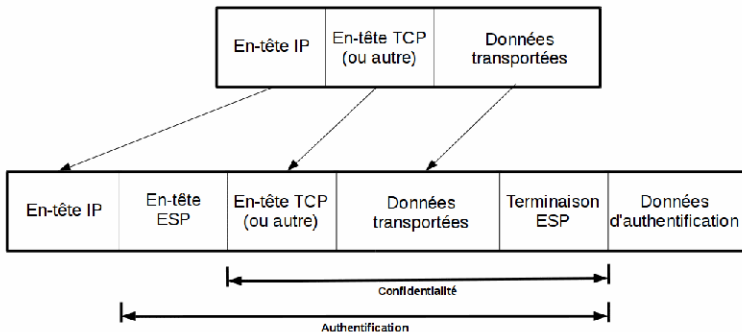
0060 1a 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d

AH en mode tunnel



Exemples avec le protocole ESP

ESP en mode transport



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter Expression... Clear Apply Enregistrer

No.	Time	Source	Destination	Protocol	Length	Info
3	4.562278	192.168.155.1	192.168.155.2	ESP	122	ESP (SPI=0x00010001)
4	4.567454	192.168.155.2	192.168.155.1	ESP	122	ESP (SPI=0x00010002)
5	5.564775	192.168.155.1	192.168.155.2	ESP	122	ESP (SPI=0x00010001)

▶ Frame 3: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)

▶ Ethernet II, Src: 52:54:00:4b:f3:0f (52:54:00:4b:f3:0f), Dst: 52:54:00:cb:65:d4 (52:54:00:cb:65:d4)

▶ Internet Protocol Version 4, Src: 192.168.155.1 (192.168.155.1), Dst: 192.168.155.2 (192.168.155.2)

▼ Encapsulating Security Payload

ESP SPI: 0x00010001 (65537)

ESP Sequence: 2

▶ Data (80 bytes)

▼ NULL Authentication

[Coco: True]

[Bac: False]

```

0000  52 54 00 cb 65 d4 52 54 00 4b f3 0f 00 45 00  RT...RT...K...E.
0010  00 6c 4a 1f 40 c0 40 32 38 ec c0 a8 5b 01 c0 a8  .J...02 8.....
0020  30 c2 00 01 30 c1 00 00 00 02 d2 ed 6a 35 98 52  .....J5.R
0030  5f df c6 1a 18 d3 2d 64 1a 93 a7 9f 1e 8e a5 51  .....d.....0
0040  a1 77 41 7a 07 c1 2a 0e be 39 aa 2c ef bh aa 7d  .A...+.S.....3
0050  ca d5 e1 c7 4a 71 92 a7 1f 35 f8 a9 ec 44 84 4f  .....Jq...5...D.0
0060  a2 f2 98 02 4c 7a c5 9d 6f b0 bd 2d 1a 1a db b5  .....7...0

```


ESP en mode transport

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter Expression... Clear Apply Save

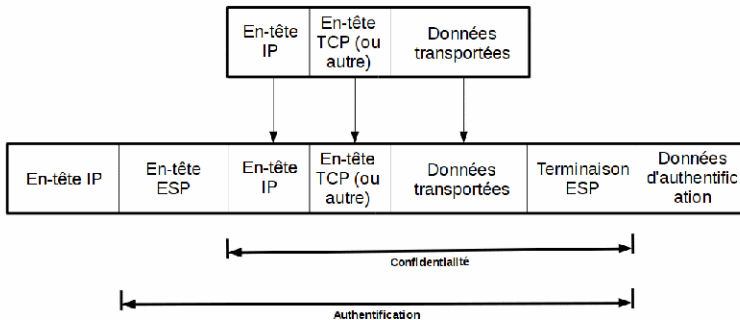
No.	Time	Source	Destination	Protocol	Length	Info
3	4.562278	192.168.155.1	192.168.155.2	ICMP	122	Echo (ping) request id=0x0915, seq=1/255, ttl=0
4	4.562436	192.168.155.2	192.168.155.1	ICMP	122	Echo (ping) reply id=0x0915, seq=1/255, ttl=0

▶ Frame 3: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
 ▶ Ethernet II, Src: 52:54:00:4b:3:6f (52:54:00:4b:3:6f), Dst: 52:54:00:cb:65:d4 (52:54:00:cb:65:d4)
 ▶ Internet Protocol Version 4, Src: 192.168.155.1 (192.168.155.1), Dst: 192.168.155.2 (192.168.155.2)
 ▼ Encapsulating Security Payload
 ESP SPI: 0x00010001 (65537)
 ESP Sequence: 2
 ESP IV: cfd6a3b9b5b5dfdf
 Pad
 ESP Pad length: 5
 Next header: ICMP (0x01)
 ▶ NULL Authentication
 ▶ Internet Control Message Protocol

```

0000 08 00 38 85 09 15 00 01 23 86 89 54 1e 87 00 00  ..8....#...T...
0010 08 09 0a 0b 0c 0e 0f 10 11 12 13 14 15 16 17  .....!$%&w
0020 18 19 1a 1b 1c 1e 1f 20 21 22 23 24 25 26 27  .....()>+.../
0030 28 29 2a 2b 2c 2e 2f 30 31 32 33 34 35 36 37  .....G1234567
0040 38 39 3a 3b 3c 3e 3f 40 41 42 43 44 45 46 47  .....
  
```

ESP en mode tunnel



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 :

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

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";
```

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



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

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.